INDEX

Srl No.	Particulars	Pages
1.	**ANNEXURE-R/1**. A copy of the notification dated 28.01.2009, through which the UIDAI was set up.	107-109
2.	**ANNEXURE-R/2**.. A copy of the Aadhaar enrollment form .	110 - 111
3.	**ANNEXURE-R/3**. A copy of the list of Registrars partnering with UIDAI .	112-114
4.	**ANNEXURE R/4.** List of 139 banks arranged in alphabetical order which have had Aadhaar beneficiary transactionsis.	115 - 118
5.	**ANNEXURE-R/5**. Summary of the cases where benefits in terms of plugging leakages, elimination of ghost and duplicate beneficiaries etc.	119 - 121.
6.	**ANNEXURE R/ 6.** Copies of Judgments in WP(C) No.196/2001, *PUCL Vs. Union of India and* Civil Appeal No.958/2013, *State of Kerala & Others Vs. President, Parents Teachers Association, SNVUP.*	122 - 153
7.	**Annexure R/7.** Copy of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.	154-158
8.	**Annexure R/8.** Copies of UIDAI Committee on Biometrics published its report titled "Biometric Design Standards for UID Applications and copy of UIDAI published a report titled "UID Enrolment Proof-of-Concept Report alongwith Glossary of Terms used.	159-253.

Annexure-R/I

Annexure 107

(TO BE PUBLISHED IN PART-I, SECTION-2 OF THE GAZETTE OF INDIA)

GOVERNMENT OF INDIA
PLANNING COMMISSION

Yojana Bhawan, Sansad Marg,
New Delhi, 28th January,2009

NOTIFICATION

No. A-43011/02/2009-Admn.I: In pursuance of Empowered Group of Ministers' fourth meeting, dated 4th November 2008, the Unique Identification Authority of India (UIDAI) is hereby constituted and notified as an attached office under aegis of Planning Commission with following terms of reference and initial core staff composition:-

COMPOSITION:

2. UIDAI shall be set up with an initial core team of 115 officials and staff as per details given below:

Post	Level	No. of Posts
UID Authority of India		
Director General & Mission Director	Additional Secretary Govt. of India	1
Deputy Director General (DDG)	Joint Secretary, Govt. of India	1
Assistant Director General (ADG)	Director, Govt. of India	1
Support Staff		
PS	PS	3
Peon	Peon	2
Driver	Driver	2
	Total Manpower	10
State /UT Units of UIDAI		
State / UT UID Commissioner	Joint Secretary, Govt. of India	35
Support Staff		
PS	PS	35
Peon	Peon	35
	Total Manpower	105
Grand Total		**115**

Role and Responsibilities of UIDAI

3 UIDAI shall have the responsibility to lay down plan and policies to implement UID Scheme, shall own and operate UID database and be responsible for its updation and maintenance on an ongoing basis

4 Implementation of UID scheme will entail, *inter alia*, following responsibilities being undertaken by UIDAI:

- Generate and assign UID to residents
- Define mechanisms and processes for interlinking UID with partner databases on a continuous basis
- Frame policies and administrative procedures related to updation mechanism and maintenance of UID database on an ongoing basis
- Co-ordinate / liaise with implementation partners and user agencies as also define conflict resolution mechanism
- Define usage and applicability of UID for delivery of various services
- Operate and manage all stages of UID lifecycle
- Adopt phased approach for implementation of UID specially with reference to approved timelines
- Take necessary steps to ensure collation of NPR with UID (as per approved strategy)
- Ensure ways for leveraging field level institutions appropriately such as PRIs in establishing linkages across partner agencies as well as its validation while cross linking with other designated agencies
- Evolve strategy for awareness and communication of UID and its usage
- Identify new partner /user agencies
- Issue necessary instructions to agencies that undertake creation of databases, to ensure standardization of data elements that are collected and digitized and enable collation and correlation with UID and its partner databases
- Frame policies and administrative procedures related to hiring / retention / mobilization of resources, outsourcing of various tasks and budgeting & planning for UIDAI and all State units under UIDAI.

5. Planning Commission shall be the nodal agency for UIDAI for providing logistics, planning and budgetary support Planning commission would provide initial office and IT infrastructure at central level.

6 Government housing will be provided to officers of UIDAI appointed on deputation from general pool of Department of Urban Development.

(Dr. Subas Pani) 28/1/10
Secretary to the Government of India

The General Manager
Govt. of India Press
Faridabad.

Copy to:

1. Secretary to the President, Rashtrapati Bhavan, New Delhi
2. Secretary to the Vice-President, Maulana Azad Road, New Delhi
3. Cabinet Secretary, Rashtrapati Bhavan, New Delhi
4. Principal Secretary to the Prime Minister, South Block, New Delhi
5. Pnvate Secretary to the Deputy Chairman, Planning Commission
6. All Ministers/Departments of Govt. of India
7. Chief Secretaries of all States/Union Territories
8. Secretary General, Rajya Sabha Secretariat, New Delhi
9. Secretary General, Lok Sabha Secretariat, New Delhi
10. Pr. Adviser (Admn & PC)/AS & FA/Adviser (C & I)/Director (GA)/DS (Admn.)
11. Pay & Accounts Officer, Planning Commission
12. Drawing & Disbursing Officer, Planning Commission
13. Accounts –I Section, Planning Commission

AADHAAR ENROLMENT / CORRECTION FORM

110

Aadhaar Enrolment is free and voluntary. Correction within 96 hours of enrolment is also free No charges are applicable for Form and Aadhaar Enrolment. In case of Correction provide your EID, Name and only that field which needs Correction.

In case of Correction provide your EID No. here : ☐☐☐☐☐☐☐☐☐☐☐☐☐☐ dd/mm/yyyy/hh:mm:ss

Please follow the instructions overleaf while filling up the form. Use capital letters only.

1	Pre-Enrolment ID :	2	NPR Receipt / TIN Number :
3	Full Name		
4	Gender Male ( ) Female ( ) Transgender ( )	5	Age Yrs/M Date of Birth Declared ☐ Verified ☐
6	Address C/o ( ) D/o ( ) S/o ( ) W/o ( ) H/o ( ) NAME		
	House No /Bldg /Apt		Street/Road/Lane
	Landmark		Area /Locality/sector
	Village / Town / City		Post Office
	District	Sub-District	State
	E-Mail	Mobile No ☐☐☐☐☐☐☐☐☐☐	PIN CODE
7	Details of : Father ( ) Mother ( ) Guardian ( ) Husband ( ) Wife ( ) *For children below 5 years Father/Mother/Guardian details are mandatory. Adults can opt to not specify this information, if they consider and want to disclose*		
	Name		
	EID / Aadhaar No ☐☐☐☐☐☐☐☐☐☐☐☐☐☐ dd/mm / yyyy / hh mm ss ☐☐☐☐☐☐☐☐☐☐☐☐☐☐		
8	I have no objection to the UIDAI sharing information provided by me to the UIDAI with agencies engaged in delivery of welfare services		YES ( ) NO ( )
9	Select One of the Below (OPTIONAL) (This data cannot be Corrected after Enrolment) ☐ I want the UIDAI to facilitate opening of a new Bank/Post Office Account linked to my Aadhaar Number and have no objection to sharing my information for this purpose ☐ I have no objection to linking my present bank account provided here to My Aadhaar number State Bank Name / Branch IFSC Code Account No		

Verification Type : Document Based ( ) Introducer Based ( ) Head of Family ( )

Select only one of the above. Select Introducer or Head of Family only if you do not possess any documentary proof of identity and / or address. Introducer and Head of Family details are not required in case of Document based Verification

10	**For Document Based** (Write Names of the documents produced. Refer back side of the form for list of valid documents)		
a. POI		b. POA	
c. DOB (Mandatory in case of Verified Date of Birth)		d. POR	
11	**For Introducer Based** - Introducer's Aadhaar No ☐☐☐☐☐☐☐☐☐☐☐☐	**For HoF Based** - Details of : Father ( ) Mother ( ) Guardian ( ) Husband ( ) Wife ( ) HoF's EID / Aadhaar No. ☐☐☐☐☐☐☐☐☐☐☐☐☐☐ dd / mm / yyyy / hh:mm:ss	

I hereby confirm the identity and address of _____ as being true, correct and accurate

Introducer / HoF's Name **Signature of Introducer / HOF**

Consent

I confirm that information (including biometrics) provided by me to the UIDAI and the information contained herein is my own and is true, correct and accurate

Applicant's signature / Thumbprint

Verifier's Stamp and Signature

(Verifier must put his / her Name, if stamp is not available)

To be filled by the Enrolment Agency only Date & time of Enrolment _____ _____

Instruction to follow while filling up the enrolment form

Field 2 **NPR NUMBER**	Resident may bring his/her National Population Register Survey Slip (if available) and fill up the column
Field 3 **NAME**	Write full name without salutations/titles. Please bring the original Proof of Identity (PoI) document. (See list A below) Variation in Resident's Name in contrast to PoI is permissible as long as the change is minor spelling only without altering the Name in PoI document. For Example if Resident's PoI reads "Preeti" then "Priti" can be recorded if Resident wants so
Field 5 **DOB / AGE**	Fill in Date of Birth in DD/MM/YY format. If exact Date of Birth is not known, approximate age in Years may be filled in the space provided. Please bring the original Proof of Date of Birth (DoB), if available. (See list D below) Declared checkbox may be selected if Resident does not have a valid proof of Date of birth document. Verified checkbox is selected where Resident has provided documents as proof of Date of Birth
Field 6 **ADDRESS**	Write complete address. Please bring the original Proof of Address (POA) document. (See list B below) Please note that the Aadhaar letter will be delivered at the given address only. • To include Parent / Guardian / Spouse name as part of the Address, select the appropriate box and enter the name of the person • Minor Corrections / Enhancements are permissible to make the address complete without altering the base address as mentioned in the POA document
Field 7 **RELATIONSHIP**	• In case of children below 5 years, it is mandatory to provide father/mother/guradian details with their Aadhaar or EID number • If the resident is not holding a Proof of Identity & using the Head of the Family Identity for enrolment, it is mandatory to provide Head of the Family's details with his/her Aadhaar or EID number. Please refer Illustration below for filling EID. Please bring the original Proof of Relationship (POR) documents (See list C below) • For other cases, it is optional for the resident to fill up the relationship details
Field 8 **CONSENT**	Resident may specifically expresses willingness / unwillingness by selecting the relevant box
Field 9 **BANK ACCOUNT**	Resident may choose to open a new Aadhaar enabled bank / POSB account or can link existing bank account to Aadhaar number. Relevant details as requested may be provided. This is an optional field
Field 10 **DOCUMENT**	Write the name of Documents for PoI and PoA. In case of Proof of Date of Birth is available then write the name of Date of Birth document. If the resident is not holding a Proof of Identity & using the Head of Family based enrolment, then write the name of Proof or Relationship document for valid list of documents please refer list of Documents below
Field 11 **INDTODUCER/HoF**	Resident who does not have POI and POA may get enrolled though an Introducer / Head of Family. Pl contact nearest enrolment centre of your Registrar for further details

List A POI documents

1. Passport
2. PAN Card
3. Ration Card / PDS Photo Card
4. Voter ID
5. Driving License
6. Government Photo ID Card / Service Photo Identity Card issued by PSU
7. NREGS Job Card
8. Photo ID issued by Recognized Educational Institute
9. Arms License
10. Photo Bank ATM Card
11. Photo Credit Card
12. Pensioner Photo Card
13. Freedom Fighter Photo Card
14. Kisan Photo Passbook
15. CGHS / ECHS Photo Card
16. Address Card having Name and Photo issued by Department of Posts
17. Certificate of Identity having photo issued by Gazetted Officer or Tehsildar on Letter Head
18. Disability ID Card / handicapped medical certificate issued by the respective State / UT Governments / Administrations

List B. POA documents

1. Passport
2. Bank Statement
3. Post Office Account Statement / Passbook
4. Ration Card
5. Voter Card
6. Driving License
7. Government Photo ID cards/ service photo identity card issued by PSU
8. Electricity Bill (not older than 3 months)
9. Water bill (Not older than 3 months)
10. Telephone Landline Bill (not older than 3 months)
11. Property [illegible]
12. Credit Card Statement (not older than 3 months)
13. [illegible]
14. Signed Letter having Photo from Bank on letter head
15. Signed Letter having Photo issued by registered Company on Letter Head
16. Signed Letter having Photo issued by Recognized Educational Instruction on letter head
17. NREGS Job Card
18. Arms License
19. Pension Card
20. Freedom Fighter Card
21. Kisan Passbook
22. CGHS / ECHS Card
23. Certificate of Address having photo issued by MP or MLA or Gazetted Officer or Tehsildar on letterhead
24. Certificate of Address issued by Village Panchayat head or its equivalent authority (for rural areas)
25. Income Tax Assessment Order
26. Vehicle Registration Certificate
27. Registered Sale / Lease / Rent Agreement
28. Address Card having Photo issued by Department of Posts
29. Caste and Domicile Certificate having Photo issued by State Govt.
30. Disability ID Card / handicapped medical certificate issued by the respective State/UT Governments/Administrations
31. Gas Connection Bill (not older than 3 months)
32. Passport of Spouse
33. Passport of Parents (in case of Minor)

List C. POR documents

1. PDS Card
2. MNREGA Job Card
3. CGHS/State Government/ECHS/ESIC Medical Card
4. Pension Card
5. Army Canteen Card
6. Passport
7. Birth Certificate issued by Registrar of Birth, Municipal Corporation and other notified local Government Bodies like Taluk, Tehsil etc
8. Any other Central/State Government issued family entitlement document

List D. DOB documents

1. Birth Certificate
2. SSLC Book/Certificate
3. Passport
4. Certificate of Date of Birth issued by Group A Gazetted Officer on Letterhead

Illustration for filling up EID No.

Acknowledgement/Resident Copy / [illegible] AADHAAR

Enrolment No / [illegible] 0008/12345/00020 Date/[illegible] 28/04/2011 15:50:16

or EID No 00081234500020 28 04 2011 15 50 16

* In instance where original documents are not available, copies attested / certified by a public notary / gazetted officer will be accepted

Registrar shall be translate this document into local language

ANNEXURE R/ 3

LIST OF REGISTRARS PARTNERING WITH UIDAI

1	Allahabad Bank
2	Bank of Baroda
3	Bank Of India
4	Bank of Maharashtra
5	Canara Bank
6	Central Bank of India
7	Civil Supplies - A&N Islands
8	CSC e-Governance Services India Limited
9	Delhi - Central DC
10	Delhi - East DC
11	Delhi - ND DC
12	Delhi - NE DC
13	Delhi - North DC
14	Delhi- South DC
15	Delhi SW DC
16	Delhi Urban Shelter Improvemen
17	Delhi- West DC
18	Delhi-NW DC
19	DENA BANK
20	Department of Information Technology Govt of Jharkhand
21	Dept of ITC Govt of Rajasthan
22	FCR Govt of Haryana
23	FCS Govt of Punjab
24	Government Of Uttar Pradesh
25	Govt of Andhra Pradesh
26	Govt of Chhattisgrah - FCSCP&L
27	Govt of Goa

28	Govt of Gujarat
29	Govt of Himachal Pradesh
30	Govt of Karnataka
31	Govt of Kerala
32	Govt of Madhya Pradesh
33	Govt of Maharashtra
34	Govt of Sikkim - Dept of Econo
35	IDBI Bank ltd
36	IGNOU
37	Indian Bank
38	Indian Overseas Bank
39	Indiapost
40	Information Technology & Communication Department
41	Jammu and Kashmir Bank
42	Jharkhand
43	Life Insurance Corporation
44	Mission Convergence - GNCT Del
45	NSDL e-Governance Infrastructure Limited
46	Oriental Bank of Commerce
47	Principal Revenue Commissioner, Dept of Revenue, Govt of MP
48	Punjab and Sind Bank
49	RDD Govt of Tripura
50	Registrar General India - BEL
51	Registrar General India BEL2
52	Registrar General India ECIL
53	Registrar General India Others
54	Registrar General of India ITI
55	State Bank of Bikaner & Jaipur
56	STATE BANK OF HYDERABAD
57	State Bank of India

58	State Bank of Mysore
59	STATE BANK OF PATIALA
60	State Bank of Travancore
61	Syndicate Bank
62	UIDAI Test Registrar
63	UIDAI-Registrar
64	Union Bank
65	United Bank of India
66	UT Of Daman and Diu
67	UT of Puducherry

Annexure R/4

LIST OF BANKS HAVING AADHAAR BENEFICIARY TRANSACTIONS

S.No.	Bank Name
1	Abhyudaya Co-operative Bank
2	AhmednagarShaharSahakari bank Maryadit
3	Allahabad Bank
4	Andhra Bank
5	Andhra PragathiGrameena Bank
6	AP Mahesh Cooperative Bank
7	ApnaSahakari Bank Ltd.
8	Assam GraminVIkash Bank
9	Axis Bank
10	BangiyaGraminVikash Bank
11	Bank of Bahrain & Kuwait
12	Bank of Baroda
13	Bank Of India
14	Bank of Maharashtra
15	BARODA GUJARAT GRAMIN BANK
16	Baroda Rajasthan KshetriyaGramin Bank
17	BARODA UTTAR PRADESH GRAMIN BANK
18	Bassein Catholic Co-Op Bank Ltd
19	Canara Bank
20	Capital Local Area Bank
21	Central Bank of India
22	CENTRAL MADHYA PRADESH GRAMIN BANK
23	Chaitanya Godavari Grameena Bank
24	City Union Bank Limited
25	Corporation Bank
26	DECCAN GRAMEENA BANK
27	Dena Bank
28	Dena Gujarat Gramin Bank
29	Development Credit Bank Limited
30	Dhanalaxmi Bank
31	DombiviliNagariSahakari Bank Ltd.
32	DurgRajnandgaonGramin Bank
33	Federal Bank
34	GopinathPatilParsikJanataSahakari Bank
35	Gurgaon Gramin Bank
36	Haryana Gramin Bank
37	HDFC Bank Ltd

38	Himachal Gramin Bank
39	ICICI Bank Ltd
40	IDBI Bank
41	Indian Bank
42	Indian Overseas Bank
43	Indusind Bank
44	ING Vysya Bank Ltd
45	JalagaonJanataSahkari Bank Ltd
46	JanakalyanSahakari Bank
47	JanataSahakari Bank Ltd.
48	JHARKAND GRAMIN BANK
49	KallappannaAwadeIchalkaranjiJanataSahakari Bank
50	Karnataka Bank Ltd.,
51	Karnataka VikasGrameena Bank
52	KarurVysa Bank
53	KashiGomtiSamyutGramin Bank
54	KaveriGrameena Bank
55	Kotak Mahindra Bank Ltd
56	Madya Bihar Gramin Bank
57	MAHARASHTRA GRAMIN BANK
58	MalwaGramin Bank
59	MANIPUR RURAL BANK
60	MEWAR AANCHALIK GRAMIN BANK
61	Mumbai District Central Co-op Bank Ltd
62	Narmada JhabuaGramin Bank
63	NKGSB CO-Op. Bank Ltd.
64	North Malabar Gramin Bank
65	NutanNagarikSahakari Bank Ltd
66	Oriental Bank of Commerce
67	PaschimBangaGramin Bank
68	PragathiGramin Bank
69	Prathama Bank
70	PuduvaiBharathiarGrama Bank
71	Punjab & Maharashtra Co-operative Bank
72	Punjab & Sind Bank
73	Punjab Gramin Bank
74	Punjab National Bank
75	RAJGURUNAGAR SAHAKARI BANK LTD
76	Ratnakar Bank
77	SaptagiriGrameena Bank
78	Saraswat Bank

79	Sarva UP Gramin Bank
80	ShreyasGramin Bank
81	Sindhudurg District Central Cooperative Bank Ltd
82	South Indian Bank
83	South Malabar Grameen Bank
84	Standard Chartered Bank
85	State Bank of Bikaner & Jaipur
86	State Bank of Hyderabad
87	State Bank of India
88	State Bank of Mauritus Ltd.
89	State Bank of Mysore
90	State Bank of Patiala
91	State Bank of Travancore
92	SUTLEJ GRAMIN BANK
93	Syndicate bank
94	Tamilnad Mercantile Bank Ltd.
95	Thane Bharat Sahakari Bank Ltd.
96	Thane JanataSahakari Bank
97	The Adarsh Cooperative Urban Bank Limited
98	The Akola District Central Cooperative Bank Ltd
99	The Andhra Pradesh state cooperative bank ltd
100	THE ARYAPURAM COOPERATIVE URBAN BANK LTD
101	THE BHARAT CO-OPERATIVE BANK LTD
102	THE BICHOLIM URBAN CO-OPERATIVE BANK LTD
103	The Catholic Syrian Bank
104	THE CHIPLUN URBAN COOPERATIVE BANK LTD
105	The Citizen Cooperative Bank Limited
106	THE COSMOS CO-OPERATIVE BANK LTD
107	THE GADCHIROLI DISTRICT CENTRAL COOPERATIVE BANK
108	THE GAYATRI COOPERATIVE URBAN BANK LTD
109	THE GOA STATE CO-OPERATIVE BANK LTD
110	The Goa Urban Co-Operative Bank Ltd.
111	The Greater Bombay Co-operative Bank Limited
112	The Himachal Pradesh State Co-operative Bank Ltd
113	THE JALGAON PEOPLES CO OP BANK LTD
114	The Jammu And Kashmir Bank Ltd
115	The Kalupur Commercial Co-Operative Bank
116	The KalyanJanataSahakari Bank Ltd.
117	THE KANGRA CENTRAL CO-OPERATIVE BANK LTD
118	The Kapol Co-Operative Bank Ltd.
119	The Karad urban Co-op Bank Ltd

120	The Lakshmi Vilas Bank Ltd.
121	THE MAPUSA URBAN COOPERATIVE BANK OF GOA LTD
122	The Mehsana Urban Co-operative Bank
123	THE MUNICIPAL CO-OP BANK LTD
124	The Nasik Merchants Cooperative Bank Ltd
125	The Pochampally Cooperative Urban Bank Ltd
126	The SahebraoDeshmukh Co-Op. Bank Ltd.
127	The Shamrao Vital Co-operative Bank
128	The VishweshwarSahakari Bank Ltd
129	THE ZOROASTRIAN CO-OPERATIVE BANK LTD
130	TJSB Sahakari Bank Ltd
131	Tripura Gramin Bank
132	UCO Bank
133	Union Bank of India
134	United Bank of India
135	UTTAR BIHAR GRAMIN BANK
136	Vijaya Bank
137	VIVEKANAND NAGRIK SAHKARI BANK MYDT
138	WAINGANGA KRISHNA GRAMIN BANK
139	YES Bank

***

Annexure R/5

CASE STUDIES RELATED TO UIDAI AND BENEFITS ACCRUED IN TERMS OF PLUGGING LEAKAGES ETC.

1. Aadhaar has been successfully used by various Central and State Governments to provide Pensions, Scholarships, MGNREGA Wages, Subsidized food etc. Some of the case studies where aadhaar has been instrumental in plugging leakages and elimination of ghost and duplicate beneficiaries have been mentioned below :-

Case 1 : UT Govt of Chandigarh : Pension Disbursement.

2. More than 20 thousand beneficiaries are covered in the schemes related to Old Age Pension, Widow Pension and Pension to Disabled Persons which also include the financial assistance given to dependents of widows.

3. After extensive enrolment campaigns, almost 3255 intended beneficiaries have not turned up either for aadhaar enrolment nor opening of bank accounts, thus giving credence to the fact that these could be ghost beneficiaries. It is estimated that approx 2.7 Crore may be saved due to these untraceable beneficiaries.

4. The end-to-end application of aadhaar is also evidenced from the fact that in March 2013, pensions amounting to Rs. 1.90 crores were directly credited to the beneficiary accounts using AePS. Till date, Rs. 1.50 Crores of pensions were disbursed through MicroATMs using aadhaar authentication services.

5. Apart from the monetary benefits, the integration of aadhaar has thus ensured effective and smooth service delivery and also enhancing transparency and efficiency, thereby eliminating delays, falsification and ghost beneficiaries. It has also ensured that the benefits reach the intended beneficiary, thereby reducing corruption. The disbursal of pensions through aadhaar enabled bank accounts have also resulted in the Financial Inclusion of the targeted beneficiaries, thereby empowering them in conducting banking transactions by leveraging aadhaar technology.

Case 2 : PDS in East Godavari District, Andhra Pradesh

6. Consequent to the Supreme Court Order related to the computerisation of the PDS on a priority basis, the aadhaar enabled payment system was implemented in this district on a pilot basis. This included identification of beneficiaries based on aadhaar number and cleansing the database of duplicates and ghosts. The instant district had an aadhaar saturation of 99% out of a total population of 52 Lakhs. The disbursal was done through Fair Price shops and use of finger print scanner at the PoS. As per the Pilot Study, the percentage of bogus cards were 12.48% which translates into 1.89 Lakh cards and with an assumption of Rs. 5,110 of subsidy per card, the savings would translate into 10,163 Lakh for the entire district, which is further assumed to increase over the years and reach 15,766.35 Lakhs. The Internal Rate of Return (IRR) works out to be an 'astounding' 116.89%. For the other stakeholder, like Central Government, the IRR was estimated at 154% and for the State Government to be 128% from this project.

Case 3 : Dilsa Project, Aurangabad

7. The Dilsa Project in Aurangabad, refers to the use of aadhaar enabled disbursement of benefits in the Aurangabad Area for the Govt Schemes like *Sanjay Gandhi Niradhar Anudhan Yojna*, *Shravan Bal Yojna*, and *Indira Gandhi National Old Age Pension Scheme*. Out of the total 22,500 which is the number of beneficiaries before the implementation, the actual number which was found to be eligible for benefits were only 11,579, thus accruing a total savings of Rs. 7.7 Crore per year.

Case 4 : Govt. of Puducherry

8. With an aadhaar saturation of 94%, covering the entire population, the DBT scheme was launched in the UT from 01.01.2013 and the beneficiaries of 16 schemes were given financial assistance through AePS. With regard to DBTL, only 58% of the total customers have seeded their aadhaar number with their bank account, and though the aadhaar saturation is 94%, it is believed that the

R16

122

ITEM NO.1 COURT NO.4 SECTION PIL

SUPREME COURT OF INDIA

RECORD OF PROCEEDINGS

WRIT PETITION (CIVIL) NO. 196 OF 2001

PEOPLE'S UNION FOR CIVIL LIBERTIES Petitioner(s)

VERSUS

UNION OF INDIA & ORS. Respondent(s)

(Regarding reports submitted by Justice D.P. Wadhwa, Retd. Judge, Supreme Court of India)

(REG. PUBLIC DISTRIBUTION SYSTEM)

I.A. Nos.90, 93, 98, 102 to 108, 110, 111 & 112 in W.P.(C) No.196/2001

(For permission on behalf of Respondent No.17 i.e. State of Maharashtra, modification and directions, intervention on behalf of West Bengal M.R. Dealers Association and All Bengal Price Shop Dealers Welfare Association, impleadment, exemption from filing O.T., directions,extension of time on behalf of State of Rajasthan, modification of Court's order dt.22.04.2009, impleadment on behalf of Karnataka State Taluka Co-operative Marketing Society Association to be impleaded as respondents and permission to file additional affidavit)

WITH

CONTEMPT PETITION (CIVIL) NO. 99/2009

123

(With Application for exemption from filing O.T.)

W.P.(C) No. 277/2010

Date:14/09/2011 These Petitions were called on for hearing today.

CORAM :

HON'BLE MR. JUSTICE DALVEER BHANDARI

HON'BLE MR. JUSTICE DEEPAK VERMA

For Petitioner(s) Mr. Colin Gonsalves,Sr.Adv.
Mr. Divya Jyoti,Adv.
Ms. Jyoti Mendiratta,Adv.

For Respondent(s) Mr. Mohan Parasaran,ASG
Mr. D.L. Chidananda,Adv.
Mr. S. Wasim A. Qadri,Adv.
Mr. A. Dev Kumar,Adv.
Ms. Sunita Sharma,Adv.
Ms. Sushma Suri,Adv.
Ms. Anil Katiyar,Adv.
Ms. Supriya Jain,Adv.
Mr. D.S. Mahra,Adv.
Mr. Sudarshan Singh Rawat,Adv.

For DDA Mr. Vishnu B. Saharya,Adv.

For M/s. Saharya & Co.,Advs.

Mr. Jana Kalyan Das,Adv.

Mr. Ranjan Mukherjee,Adv.
Mr. S.C. Ghosh,Adv.

Ms. Hemantika Wahi,Adv.
Ms. Suveni Banerjee,Adv.

Mr. D.K. Goswami,Adv.
Mr. Shirish Kr. Mishra,Adv.

Mr. Pragyan P. Sharma,Adv.
Mr. Siddhartha Lodha,Adv.
for Mr. P.V. Yogeswaran,Adv.

Mr. H.P. Raval,ASG
Ms. Indra Sawhney,Adv.

Dr. Manish Singhvi,AAG,Raj.
Mr. Devanshu Kumar Devesh,Adv.
Mr. Irshad Ahmad,Adv.
Mr. Milind Kumar,Adv.

Mr. A. Mariarputham,Adv.Gen,
Mrs. Aruna Mathur,Adv.
Mr. Avneesh Arputham,Adv.
Mr. Yusuf Khan,Adv.
For M/s. Arputham Aruna & Co.,Advs.

Mr. Riku Sarma,Adv.

Mr. Navnit Kumar,Adv.

for M/s. Corporate Law Group,Advs.

Ms. Rachana Srivastava,Adv.

Mr. Ranchi Daga,Adv.

Mr. Krutin Joshi,Adv.

Mr. Manoj Saxena,Adv.

Mr. Mayank Nigam,Adv.

Mr. T.V. George,Adv.

Ms. Kamini Jaiswal,Adv.

Mr. Shish Pal Laler,Adv.

Mr. Khwairakpam Nobin Singh,Adv.

Mr. Sapam Biswajit Meitei,Adv.

Mr. Ranjan Mukherjee,Adv.

Mr. Jatinder Kumar Bhatia,Adv.

Mr. R. Sundaravaradhan,Sr.Adv.

Mr. V.G. Pragasam,Adv.

Mr. S.J. Aristotle,Adv.

Mr. Prabu Ramasubramanian,Adv.

Mr. G.V. Rao,Adv.

Mr. Ravi Prakash Mehrotra,Adv.

Mr. Gopal Singh,Adv.
Mr. Manish Kumar,Adv.
Mr. Chandan Kumar,Adv.

Mr. Bikas Kar Gutpa,Adv.
Mr. Abhijit Sengupta,Adv.

Mr. Rituraj Biswas,Adv.

Mr. Manish Pitale,Adv.
Mr. Wasi Haider,Adv.
For Mr. C.S. Ashri,Adv.

Mr. Soumitra G. Chaudhuri,Adv.
Mr. Tara Chandra Sharma,Adv.

Mr. Anil Shrivastav,Adv.
Mr. Ritu Raj Biswas,Adv.

Mr. Edward Belho,Adv.
Mr. P. Athuimei R. Naga,Adv.
Mr. K. Enatoli Sema,Adv.
Mr. Nimshim Vashum,Adv.

Mr. T. Harish Kumar,Adv.
Mr. V. Vasudevan,Adv.

Mr. Sanjiv Sen,Adv.
Mr. Prashant Kumar,Adv.

127

Mr. P. Parmeswaran,Adv.
Mr. Ujjal Banerjee,Adv.

Mr. Atul Jha,Adv.
Mr. D.K. Sinha,Adv.

Mr. G.V. Chandrashekhar,Adv.
Mr. N.K. Verma,Adv.
Ms. Anjana Chandrashekar,Adv.

Mr. Gopal Prasad,Adv.
Mr. Sarbojit Dutta,Adv.

Mr. D. Mahesh Babu,Adv.
Mr. Ramesh Allank i,Adv.
Mr. Savita Dhande,Adv.
Mr. V. Pattabhi,Adv.

Mr. Sunil Fernandes,Adv.
Mr. Suhaas Joshi,Adv.
Ms. Astha Sharma,Adv.

Mr. Ramesh Babu M.R.,Adv.

Ms. Anuradha Rustagi,Adv.
Ms. D. Bharathi Reddy,Adv.

Mr. Sanjay R. Hegde,Adv.
Mr. Ramesh Kr. Mishra,Adv.

Ms. Sumita Hazarika,Adv.

Mr. K.K. Mahalik,Adv.

Mr. Ajay Pal,Adv.

Mr. Manjit Singh,Adv.

Mr. Kamal Mohan Gupta,Adv.

Ms. A. Subhashini,Adv.

Mr. Gopal Singh,Adv.

Mr. Rituraj Biswas,Adv.

Mr. Kuldip Singh,Adv.

Mr. R.K. Pandey,Adv.

Mr. H.S. Sandhu,Adv.

Mr. K.K. Pandey,Adv.

Mr. Mohit Mudgil,Adv.

Mr. Ravindra Keshavrao Adsure,Adv.

Ms. Bina Madhavan,Adv.

Mr. Prashant Kumar,Adv.

Mr. Vishwajit Singh,Adv.

Mr. Sanjay V. Kharde,Adv.

Ms. Asha G. Nair,Adv.

Mr. K.V. Mohan,Adv.

Mr. Rajesh Srivastava,Adv.

Mrs. Promila,Adv.
Mr. S. Thananjayan,Adv.

Mr. Anuvrat Sharma,Adv.

Mr. K.N. Madhusoodhanan,Adv.
Mr. R. Sathish,Adv.

Mr. Naushad Ahmad Khan,Adv.
Mr. Rajesh Kumar Verma,Adv.
for Mr. R.C. Kaushik,Adv.

Mr. Pradeep Misra,Adv.

Mr. Venkateswara Rao Anumolu,Adv.

Mr. Bikas Upadhyay,Adv.
Mr. B.S. Banthia,Adv.

Dr. Aman Hingorani,Adv.
Ms. Priya Hingorani,Adv.

Mr. G. Prakash,Adv.
Ms. Beena Prakash,Adv.
Mr. V. Senthil,Adv.

Mr. Navneet Kumar,Adv.

Mr. Anil Kumar Jha,Adv.

Mr. Vikas Mehta,Adv.

Mr. Pramod Swaroop,Sr.Adv.
Mr. Raj Kumar Gupta,Adv.
Mr. Rajiv Dubey,Adv.
Mr. Kamlendra Mishra,Adv.

Mr. Naresh K. Sharma,Adv.

Mr. Anis Suhrawardy,Adv.

Mr. Shivaji M. Jadhav,Adv.

Mr. Suresh Chandra Tripathy,Adv.

Mr. Navin R. Nath,Adv.

UPON hearing counsel the Court made the following

ORDER

The High Powered committee headed by Justice D.P. Wadhwa, Retired Judge of this Court, has submitted a Preliminary Report on Computerization of Public Distribution System. In the recommendations of the Report it is mentioned that Computerization of PDS consists of primarily three components i.e. creating a updating beneficiary

database, stocks management from FCI till FPS and sale of commodities at Fair Price Shops. In order to make PDS effective it is important that the delivery and management system is transparent. The citizen participation for social audit can play a crucial role in ensuring effectiveness of the system. In order to implement this system across the country, the following actions are suggested by the Committee:

1. End to end computerization of PDS may be considered in two parts and following prioritisation of the Implementation Strategy may be followed:

Component I:- Diversions, leakages, delays in allocation and transportation, inappropriate distribution of foodgrains to fair price shops go unchecked because of lack of visibility of this information in the public domain.

Computerization of complete supply chain management up to the shop level and availability of this information on a Transparency Portal in public domain is to be accorded the highest priority. The portal should have different dashboards catering to the information needs of all the stakeholders.

Component II:- Electronic authentication of delivery and payments at the fair price shop level. In order to ensure that each card holder is getting his due entitlement computerization has to reach literally every doorstep and this could take long. Moreover several States have already started implementing smart cards, food coupons etc. which have not been entirely successful.
Reengineering these legacy systems and replacing it with online Aadhaar authentication at the time of foodgrain delivery will take time. This is therefore proposed ascomponent II.

2. Department of Food & Public Distribution is directed to immediately issue guidelines to all the States for end to end computerization of TPDS.

3. Government of India shall ensure that State Governments prepare a time bound action plan for completing the process of computerization. These action plan will be implemented keeping the timelines in mind and will be regularly submitted before the Hon'ble Supreme Court.

4. States/UTs should take up End to End computerization of TPDS as a top priority and should appoint a dedicated nodal officer to monitor the projects related to TPDS computerization.

5. States/UTs maybe encouraged to include the PDS related KYR+ field in the date collection exercise being undertaken by various Registrars across the country as part of the UID (Aadhaar) enrolment.

6. Digitization of beneficiary data and a centralized database with clear process of data updation to be put in place by States in a time bound manner.

7. Dissemination of information about availability of foodgrains through SMS to the pre-identified individuals in the local community to enable social audit. The system could also provide stock position at a specific location on demand. The information related to stock availability using latest technological inter face should be made available in a public domain.

8. Single unified information system should be developed to meet the above mentioned requirements that would help to achieve certain basic level of transparency in PDS. For this states should arrange training programs for field functionaries and FP dealers.

9. Chhattisgarh model of computerization for PDS System; (A note on the computerization of PDS in the State of Chhattisgarh is annexed hereto as Annexure II) which primarily cater to the computerization upto the shop level was also deliberated upon and discussed in the HPC. It was decided that the Chhattisgarh model may be adopted for component 1 and component 2 maybe done on the similar lines of the Gujarat model of computerization.

The Chhattisgarh model may be implemented in all the States within a maximum period of three months. However, some State Governments like Government of Gujarat which is following Component 2, or other States which may be at the advanced stage of following some other model, such States may continue to follow the same so long as it is fulfilling the end objectives of completing the computerization. (A note on the computerization of PDS in the State of Gujarat is annexed hereto as Annexure III).

10. As the process of end to end computerization is expected to be a sizable exercise, to complete it in a mission mode, a separate and dedicated institutional mechanism is to be incorporated to look after the progress of computerization of PDS. This institution must have active participation of all stake holders including the State Governments. As PDS is implemented by the State by the State Governments and supported by Government of India, role of State Government in this body will be helpful in getting required support from the State Governments.

11. Information related to stock availability, movement and date quantity of stocks supplied to FPS should be made available in public domain by using latest technological interface like SMSs/website or other means.

12. As far as possible, state governments should be directed to link the process of computerization of Component-2 with AADHAR Registration. This will help in streamlining the process of biometric collection as well as authentication. States/UTs may be encouraged to include the PDS related KYR+ field in the data collection exercise being undertaken by various Registrars across the country as part of the UID (Aadhar) enrolment.

13. An effective grievance redressal mechanism should be strictly enforced based on SMS/email and other suitable technology. Government of India should ensure that this mechanism is put in place in all the states. State/UTs should create effective grievance redressal mechanism where use of mobile based SMS/email can be used for timely resolution of the citizen/beneficiary grievance. A four digit toll free number may be established in all the States for grievances registration and redressal thereof.

14. Government of India will ensure that the computerization operation is provided necessary infrastructure and financial support. This needs to be completed in a time bound manner and the institution mechanism so created shall be completely responsible for meeting the timelines. Government of India with the help of state government will ensure that the institution has sufficient infrastructure and finances to complete the computerization in a time bound manner.

15. While this complete process is expected to take some time, in the meantime, following action may immediately be taken.

a. State Governments will ensure door step delivery of food grain for the ration shops in a time bound manner and shall ensure that information related to movement and availability of food grain is available in public domain.

b. A PDS Public Information portal may be made which will have information related to complete public distribution system. In addition to other information, it should also have the information of date and quantity of food grain supplied to the fair price shop every month for all the shops.

c. The digitized database of ration cards will be put up in the public domain including on the websites.

d. State should make necessary amendments to make the fair price shop financially viable.

e. A four digit toll free number may be established in all the States for grievances registration and redressal thereof.

f. All the State governments will ensure that required allocation reaches the fair price shop before 1st day of the month and this information should be available on the transparency portal.

g. A drive can be started to eliminate the fake and ghost ration cards. A comparison with data available with other departments like election, census etc. gives the quick estimates about the bogus cards. It was seen that at some places, units in the ration cards exceed even the populations of the area. These practices should be checked

immediately. This can also be linked up with the Socio Economic Census in Rural Areas which is expected to be completed shortly within this year itself.

h. Government of India shall ensure that all the state governments prepares a time bound action plan for complete computerization of PDS system within three months' time. Strict deadlines may be fixed in the action plan.and these will be submitted before Hon'ble Supreme Court within three months period.

i. All above steps may be completed within three months time.

We have discussed the recommendations of the High Powered Committee on Computerization with the learned counsel for the petitioner and the learned Additional Solicitor General of India. The Government of India has agreed in principle to implement these recommendations as expeditiously as possible. We request Mr. Parasaran, learned Additional Solicitor General to ensure that the process of computerization is completed as expeditiously as possible. He may help in coordinating with the High Powered Committee and other concerned authorities and individuals.

We direct the Chief Secretaries of various States to indicate, within two weeks, as to how much additional foodgrains is required for the poorest districts in their States and allocation of foodgrains would be made within two weeks thereafter. We further direct the Chief Secretaries to ensure that whatever foodgrains are allocated, the same be lifted by them within two weeks thereafter. The allocation of goodgrains to be made out of five million tonnes additionally allocated.

137

We request the High Powered Committee to hear all the parties and decide whether the foodgrains is required to be distributed at AAY rates or BPL rates and the decision of the High Powered Committee would be binding on all concerned and would be implemented forthwith.

We request the High Powered Committee to decide this issue as expeditiously as possible and we direct the parties to appear before the High Powered Committee on 20th September, 2011. In case the Chief Secretaries of various States do not respond within two weeks, as directed above, it would be presumed that, that particular State does not require additional foodgrains at AAY or BPL rates.

Learned counsel appearing on behalf of the Planning Commission submits that the affidavit to be filed in pursuance of the directions of this Court, has gone to the office of the Prime Minister for vetting and the same would be filed within a week. Reply to that affidavit, if any, be filed within one week thereafter.

All those States who have not filed their affidavits may file the same within two weeks from today.

List this matter for further directions on 11th October, 2011.

(A.S. BISHT)
COURT MASTER

(SHASHI BALA VIJ)
ASSISTANT REGISTRAR

138

Reportable

IN THE SUPREME COURT OF INDIA

CIVIL APPELLATE JURISDICTION

CIVIL APPEAL NO. 958 OF 2013
(Arising out of SLP(C) No.9162 of 2011)

State of Kerala and others .....
Appellants

Versus

President, Parent Teacher Assn. SNVUP and others ... Respondents

JUDGMENT

K.S. Radhakrishnan, J.

1. Leave granted.

2. We are in this appeal concerned with the question whether the High Court was justified in directing the Secretary, General Education Department of the State of Kerala to get the verification of the actual students' strength in all the aided

schools in the State with the assistance of the police and to take appropriate action.

3. The Assistant Educational Officer (AEO), Valappad had fixed the staff strength of S.N.V.U.P. School, Thalikulam for the year 2008-09 based on the visit report of High School Association (SS), GHS Kodakara as per Rule 12 of Chapter XXIII of Kerala Education Rules (KER). Later, based on a complaint regarding bogus admissions and irregular fixation of staff for the year 2008-09 by the AEO, the Super Check Cell, Malabar Region, Kozhikode made a surprise visit in the school on 17.09.2008 and physically verified the strength of the students and noticed undue shortage of attendance on that day. The strength verified by the Super Check Cell was not sufficient for allowing the divisions and posts sanctioned by the AEO. The Head Master of the School, however, stated in writing that the shortfall of attendance on the day of inspection was due to "Badar Day" of Muslim community and due to distribution of rice consequent to that. In order to confirm the genuineness of the facts stated by the Head Master, the Cell again visited the school on 16.12.2008. Verification could not be

done on that day, hence the Cell again visited the school on 02.02.2009 and physically verified the students' strength. On that day also, there were large number of absentees as noticed on 17.09.2008. On verification of attendance register, it was found that the class teachers of respective classes had given bogus presence to all students on almost all the days. Enquiry revealed that the school authorities had obtained the staff fixation order for the year 2008-09 through bogus recordical admissions.

4. The Director of Public Instructions (DPI), Thiruvananthapuram consequently issued a notice dated 07.05.2009 to the Manager of the School of his proposal to revise roll strength and revision of staff strength by reducing one division each in Std. I, II, IV to VII and 2 divisions in Std. III and consequent posts of 5 LPSAs, 3 UPSAs in the school during the year 2008-09. The Manager of the school responded to the notice vide representation dated 27.05.2009 stating that Super Check Officials did not record the attendance particulars of the students in the visit record and had tampered with the attendance register. The Manager had also pointed out that the Headmaster was not

responsible to compensate the loss suffered by the Department by way of paying salary to the teachers who had worked in the sanctioned posts. Further, it was also pointed out that the staff fixation should not be done within the academic year and re-fixation was not permissible as per Rule 12E(3) read with Rule 16 of Chapter XXIII, KER and requested not to reduce the class divisions.

5. The DPI elaborately heard the lawyers appearing for the Headmaster and the Manager of the school, affected teachers as well as the officials of the Super Check Cell. Having heard the submissions made and perusing the records made available, the DPI found that the staff fixation of the school for the year 2008-09 was obtained through bogus admissions and misrepresentation of facts. DPI noticed that the roll strength during the year 2008-09 was 1196. There were 404 absentees on the first visit of the Cell on 17.09.2008. The Super Check Cell again visited the school on 16.12.2008 and 02.02.2009 and it was found that among 404 students absent on the first day, 179 names were bogus and irregular retentions. The physical presence of 179 students could

not be verified on all the three occasions. DPI, therefore, passed an order revising the staff fixation of the school for the year 2008-09 as per Rule 12(3) read with Rule 16 of Chapter XXIII of KER. Consequently, the total number of divisions in the school was reduced to 23 from 31. In the Order dated 08.09.2009, the DIP had stated as follows:

> "The Headmaster is responsible for the admission, removals, and maintenance of records and for the supervision of work of subordinates. It is the duty of the verification officer to verify the strength correctly and to unearth the irregularities. Due to the irregular fixation of staff, the State exchequer has incurred additional and unnecessary expenditure by way of pay and allowances for 8 teachers and expenditure incurred in connection with payment of various scholarships, lump-sum grant, noon-feeding, free books etc to the bogus students. These loss sustained to the Government will be recovered from the Headmaster of the school who alone is responsible for all the above irregularities."

6. The DPI also directed to take further action to fix the liabilities and recover the amount from the Headmaster under intimation to DPI and the Super Check Officer, Kozhikode. The Headmaster and Manager of the school, aggrieved by the above-

mentioned order, filed a revision petition before the State Government. The High Court vide its judgment dated 7.12.2009 in Writ Petition (C) No. 35135 of 2009 directed the State Government to dispose of the revision petition.

7. The higher level verification was also conducted in the school with regard to the staff fixation for the year 2009-10 and on verification, it was found that many of the students in the school records were only bogus recordical admissions. Following that, the AEO issued staff fixation order for the year 2009-10 vide proceedings dated 27.03.2010.

8. Meanwhile, the President of the Parent Teachers Association (Respondent No.1 herein) filed WP (C) No. 12285 of 2010 before the High Court seeking a direction to the AEO to reckon the entire students present in the school on the 6th working day and higher level verification of District Education Officer (DEO) on 13.01.2010 for the purpose of staff fixation for the year 2009-10 and also for a declaration that the exclusion of the students who were present on the day of higher level verification on 13.01.2010 from the

staff fixation order 2009-10 was illegal and also for other consequential reliefs.

9. Learned Single Judge of the High Court dismissed the Writ Petition on 07.04.2010 stating that the Parent Teachers Association have no locus standi in challenging the staff fixation order. The judgment was challenged in W.A No.1195 of 2010 by the President, Parent Teachers Association before the Division Bench of the High Court and the Bench passed an interim order on 14.07.2010. The operative portion of the same reads as follows:-

> "The inspection team has recorded that as many as 179 students whose names and particulars are furnished, represent bogus admissions for record purposes. If admission register is manipulated by recording bogus admissions in the name of non-existing students or students of other institutions, we fell criminal action also is called for against the school authorities. Since appellant has denied the findings in the inspection report, we fell a police enquiry is called for the in the matter. We, therefore, direct the Superintendent of Police, Thrissur to constitute a team of Police Officers to go through Ext.P1, verify the registered maintained by the school authorities, take the addresses as shown in the school records and conduct field enquiry as to whether the students are

> real persons and if so, whether they are really studying in this school or elsewhere. In other words, the result of the enquiry is to confirm to this court whether the students whose names are in the record of the school are real and if so, whether they are students in this school or any other school."

The Bench also directed to the Superintendent of Police to submit his report within one month.

10. The Superintendent of Police, following the direction given by the High Court, constituted a team under the leadership of the Circle Inspector of Police, Valappad and the team conducted detailed enquiry in respect of all the matters directed to be examined by the police. The Superintendent of Police submitted the report dated 20.09.2010 which reads as follows:

> "On the enquiry about the 187 students (179+8) which were alleged as bogus admissions as per Ext.P1, it is revealed that only 72 students were studied in S.N.V.U.P. School during the period 2008-09 and 80 students were studied in some other schools. The addresses of 23 students have not been traced out even with the help of postman of the concerned area. On the enquiry it is also revealed that 4 students vide the admission Nos. 13008, 11875, 12883 and 13876 mentioned in Ext.P1, have not been studied anywhere during that period.

The details of the 187 students, revealed in the enquiry are mentioned below:-

1. Actual No. of students studied in SNVUP School, Thalikulam during 2008-2009	72
2. No. of Students studied in some other schools	80
3. No. of students whose address have not been trace out	23
4. No. of students have not been studied anywhere	04
5. No. of students removed from the rolls. Immediately after strength inspection	08
Total	187

The report of the enquiry, submitted by the Circle Inspector of Police, Valappad showing the details of each students is also produced herewith."

11. The Division Bench of the High Court after perusing the report submitted by the Superintendent of Police found that neither the finding of the DPI based on inspections by Super Check Cell nor the claim of the Parent Teachers Association was correct since the police had found that at least 72 out of 187

students declared bogus by the DPI were real students of the school. The High Court, therefore, concluded manipulation by the school management was obvious, though not to the extent found by the Super Check Cell based on which DPI had passed the impugned order. The Division Bench expressed anguish that the management had included 80 students studying in other schools as students of the present school. It was also noticed that as many as 23 students could not be traced by the police with the help of the postman, were also included in the register.

12. The Division Bench concluded that since the Super Check Cell, the Education Department lacked the investigating skill or the authority to collect information from the field, it would be appropriate that the verification of actual students in all the aided schools in the State would be done through the police. Holding so, the High Court gave the following direction:

> "We, therefore, feel as in this case Police should be entrusted to assist the Education Department by conducting enquiry about the actual and real students studying in every aided school in the State and pass on the same to the Education Department for them to

fix or re-fix the staff strength based on the data furnished by the Police. We, therefore, direct the Secretary, Department of Education, to get verification of the actual students studying in all the aided schools in the State done through the police authorities and take appropriate action. It would be open to the Government to consider photo or finger identification of the students for avoiding manipulation in the school registers. The Government is directed to complete the process by the end of this academic year and file a report in this court."

13. The State of Kerala, aggrieved by the various directions given by the Division Bench, has preferred this appeal. Ms. Liz Mathew, learned counsel appearing for the State of Kerala submitted that the High Court was not justified in giving a direction to the Secretary, Education Department in entrusting the task to State Police for verification of actual students' strength in all the aided schools, while the enquiry is being conducted by the Education Department. Learned counsel submitted that Kerala Education Act and Rules did not prescribe any mechanism for conducting enquiries by the police at the time of staff fixation. The method to be adopted in the fixation of staff in various schools is prescribed under Chapter XXIII of KER and police have

no role. The Rules empower the AEO, the DEO and the Super Check Cell etc. to conduct enquiries but not by the police. Learned counsel also pointed out that the presence of the police personnel in the aided schools in the States would not only cause embarrassment to the students studying in the school but would also cast wrong impression on the minds of the students about the conduct of their Headmaster, teachers and staff of the school.

14. We notice that the State itself had admitted in the petition that there should be a better mechanism to ascertain the number of students in the aided schools which could be done by finger printing or any other modern system so that the students could be properly identified and staff fixation could be done on the basis of relevant data. We, therefore, directed the State to evolve a better mechanism to overcome situations like the one which has occurred in the school. Fact finding authorities have categorically found that the school authorities had made bogus admissions and made wrong recording of attendance which led to the irregular and illegal fixation of staff strength of the school for the years 2008-09 and 2009-10.

150

15. An additional affidavit has been filed by the State of Kerala stating that the Government after much thought and deliberations formulated a scientific method to resolve the issue emanating from staff fixation orders every year. The affidavit says that the number of students in the school can be determined through Unique Identification Card (UID) technology and the number of divisions could be arrived at on the basis of revised pupil teacher ratio. Further, it is also pointed out that after implementation of UID as a part of scientific package, the government will remand the matter of identification of bogus admission to the DPI for considering issues afresh after corroborating the findings of Super Check Cell with UID details of the students. The State has issued a circular No. NEP (3) 66183/2011 dated 12.10.2011 which, according to the State, would take care of such situations happening in various aided schools in the State.

16. We are of the view even though the Division Bench was not justified in directing police intervention, the situation that has unfolded in this case is the one that we get in many aided schools

in the State. Many of the aided schools in the State, though not all, obtain staff fixation order through bogus admissions and misrepresentation of facts. Due to the irregular fixation of staff, the State exchequer incurs heavy financial burden by way of pay and allowances. The State has also to expend public money in connection with the payment of various scholarships, lump-sum grant, noon-feeding, free books etc. to the bogus students.

17. A great responsibility is, therefore, cast on the General Education Department to curb such menace which not only burden the State exchequer but also will give a wrong signal to the society at large. The Management and the Headmaster of the school should be a role model to the young students studying in their schools and if themselves indulge in such bogus admissions and record wrong attendance of students for unlawful gain, how they can imbibe the guidelines of honesty, truth and values in life to the students. We are, however, of the view that the investigation by the police with regard to the verification of the school admission, register etc., particularly with regard to the admissions of the students in the aided schools will give a wrong

signal even to the students studying in the school and the presence of the police itself is not conducive to the academic atmosphere of the schools. In such circumstances, we are inclined to set aside the directions given by the Division Bench for police intervention for verification of the students' strength in all the aided schools.

18. We are, however, inclined to give a direction to the Education Department, State of Kerala to forthwith give effect to a circular dated 12.10.2011 to issue UID Card to all the school children and follow the guidelines and directions contained in their circular. Needless to say, the Government can always adopt, in future, better scientific methods to curb such types of bogus admissions in various aided schools.

19. We, however, find no reason to interfere with the direction given by the DPI to take further action to fix the liabilities for the irregularity committed in the school for the years 2008-09 and 2009-10, for which the appeal is pending before the State Government. The State Government will consider the appeal and

take appropriate decision in accordance with law, if it is still pending. Appeal is allowed as above without any order as to costs.

.....J.
(K.S. Radhakrishnan)

.....J.
(Dipak Misra)

New Delhi,
February 6, 2013

Annexure - R/7

154

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(Department of Information Technology)
NOTIFICATION
New Delhi, the 11th April, 2011

G.S.R. 313(E).—In exercise of the powers conferred by clause (ob) of sub-section (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely.--

1. **Short title and commencement** — (1) These rules may be called the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

(2) They shall come into force on the date of their publication in the Official Gazette.

2. **Definitions** — (1) In these rules, unless the context otherwise requires,--

(a) "Act" means the Information Technology Act, 2000 (21 of 2000);

(b) "Biometrics" means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', "facial patterns', 'hand measurements' and 'DNA' for authentication purposes;

(c) "Body corporate" means the body corporate as defined in clause (i) of explanation to section 43A of the Act;

(d) "Cyber incidents" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;

(e) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;

(f) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;

(g) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act,

(h) "Password" means a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information;

(i) "Personal information" means any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

3. Sensitive personal data or information.— Sensitive personal data or information of a person means such personal information which consists of information relating to,—

(i) password;

(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ,

(iii) physical, physiological and mental health condition,

(iv) sexual orientation;

(v) medical records and history,

(vi) Biometric information;

(vii) any detail relating to the above clauses as provided to body corporate for providing service, and

(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules

4. Body corporate to provide policy for privacy and disclosure of information.— (1) The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. Such policy shall be published on website of body corporate or any person on its behalf and shall provide for—

(i) Clear and easily accessible statements of its practices and policies;

(ii) type of personal or sensitive personal data or information collected under rule 3,

(iii) purpose of collection and usage of such information,

(iv) disclosure of information including sensitive personal data or information as provided in rule 6,

(v) reasonable security practices and procedures as provided under rule 8

5. Collection of information.— (1) Body corporate or any person on its behalf shall obtain consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

(2) Body corporate or any person on its behalf shall not collect sensitive personal data or information unless —

(a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and

(b) the collection of the sensitive personal data or information is considered necessary for that purpose

(3) While collecting information directly from the person concerned, the body corporate or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of —

(a) the fact that the information is being collected,

(b) the purpose for which the information is being collected;

(c) the intended recipients of the information, and

(d) the name and address of —

(i) the agency that is collecting the information, and

(ii) the agency that will retain the information

(4) Body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force

(5) The information collected shall be used for the purpose for which it has been collected

(6) Body corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible:

Provided that a body corporate shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by

the provider of information to such boy corporate or any other person acting on behalf of such body corporate

(7) Body corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate In the case of provider of information not providing or later on withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought

(8) Body corporate or any person on its behalf shall keep the information secure as provided in rule 8

(9) Body corporate shall address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. For this purpose, the body corporate shall designate a Grievance Officer and publish his name and contact details on its website The Grievance Officer shall redress the grievances or provider of information expeditiously but within one month ' from the date of receipt of grievance

6. Disclosure of information.— (1) Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation

Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person

(2) Notwithstanding anything contain in sub-rule (1), any sensitive personal data on Information shall be disclosed to any third party by an order under the law for the time being in force

(3) The body corporate or any person on its behalf shall not publish the sensitive personal data or information.

(4) The third party receiving the sensitive personal data or information from body corporate or any person on its behalf under sub-rule (1) shall not disclose it further

7. Transfer of information.-A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer

8. Reasonable Security Practices and Procedures.— (1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies

(2) The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1).

(3) Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation

(4) The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried cut by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource

Unique Identification Authority of India
Planning Commission,
Yojana Bhavan,
Sansad Marg,
New Delhi 110001

Biometrics Design Standards For UID Applications

Version 1.0
December 2009

Prepared by: UIDAI Committee on Biometrics

CONTENTS

1 Executive Summary

The Unique Identification Authority of India (UIDAI) was set up by the Govt. of India on 28 January 2009. The purpose of the UIDAI is to issue Unique Identification numbers to all residents in the country. The Authority set up a Biometrics Standards Committee in order to frame biometrics standards for use by the UIDAI and its partners. The first deliverable of the Committee was to frame biometric standards based on existing national and international standards, with the consensus of various government stakeholders. The second deliverable was to recommend appropriate biometrics parameters to achieve the UIDAI's mandate. The second goal of the Committee encompasses best practices, expected accuracy, interoperability, conformity and performance in biometrics standards.

After reviewing international standards and current national recommendations, the Committee concluded that the ISO 19794 series of biometrics standards for fingerprints, face and iris set by the International Standards Organization are the most suitable. These standards are widely accepted, and best embody previous experiences of the US and Europe with biometrics. The standards framed for the UIDAI are accordingly, fully compliant with the respective ISO standards, and are given in Sections 7 through 11.

The Committee notes that Face is the most commonly captured biometric, and frequently used in manual checking. However, stand-alone, automatic face recognition does not provide a high level of accuracy, and can only be used to supplement a primary biometric modality. Fingerprinting, the oldest biometric technology, has the largest market share of all biometrics modalities globally. The fingerprint industry also has a variety of suppliers and a base of experienced professionals necessary to implement the unique identity management solution at the scale that India requires. Based on these factors, the Committee recognises that a fingerprints-based biometric system shall be at the core of the UIDAI's de-duplication efforts.

The Committee however, is also conscious of the fact that de-duplication of the magnitude required by the UIDAI has never been implemented in the world. In the global context, a de-duplication accuracy of 99% has been achieved so far, using good quality fingerprints against a database of up to fifty million. Two factors however, raise uncertainty about the accuracy that can be achieved through fingerprints. First, retaining efficacy while scaling the database size from fifty million to a billion has not been adequately analyzed. Second, fingerprint quality, the most important variable for determining de-duplication accuracy, has not been studied in depth in the Indian context.

The Committee therefore held extensive meetings and discussions with international experts and technology suppliers. A technical sub-group was also formed to collect Indian fingerprints and analyze quality. Over 250,000 fingerprint images from 25,000 persons were sourced from districts of Delhi, UP, Bihar and Orissa. Nearly all the images were from rural regions, and were collected by different agencies using different capture devices, and through different operational processes. The analysis reported in Section 12.4 and the associated Annexure show that the UIDAI could obtain fingerprint quality as good as seen in developed countries, provided that proper operational procedures are followed and good quality devices are used. On the other hand there is

Book 2
Book 2
Book 2
Book 2
Book 2

Book 2
Book 2
Book 2
Book 2

Book 2
Book 2
Book 2
Book 2
Book 2
Book 2
Book 2
Book 2
Book 2

Book 2
Book 2
Book 2

Book 2

Book 2
Book 2
Book 2
Book 2
Book 2
Book 2
Book 2

Book 2
Book 2
Book 2
Book 2
Book 2
Book 2
Book 2
Book 2
Book 2
Book 2

Book 2
Book 2
Book 2
Book 2
Book 2
Book 2

data to suggest that quality and therefore the accuracy drops precipitously if attention is not given to operational processes.

The demographic data (non-biometric data) is also used for improving de-duplication processes. It reduces the amount of manual labor required to establish genuine duplicates from a possible list of duplicate matches.

Further, it has also been observed that Iris, which for a long period of time was under the proprietary domain, is emerging as an important biometric modality after fingerprint and face. The accuracy and speed of iris-based systems currently deployed is promising and may be feasible in large-scale de-duplication systems.

Finally, it is possible to combine multiple biometric modalities including multiple fingerprints to increase overall de-duplication accuracy.

Recommendations

Based on the above deliberations, the Committee makes the following principal recommendations:

1. The Committee expects that the UIDAI could achieve at least 95% de-duplication accuracy using moderately good fingerprint images for a database size of 1 billion. Empirical image quality data of Indian ground conditions clearly show that such accuracy is achievable. In the global context, a de-duplication accuracy of 99% has been demonstrated to be achievable using good quality fingerprints against a database of up to fifty million.
2. In order to capture moderately good fingerprint images, a few simple but critical techniques during enrolment should be consistently followed, failing which material reduction in accuracy would occur. Manual and automated monitoring should be utilized to ensure consistent use of good enrolment practices.
3. In view of the above, the Committee feels that the UIDAI should collect photograph and ten fingerprints as per ISO standards described in Sections 8, 9 and 10.
4. Biometrics data are national assets and must be preserved in their original quality. In other words, quality must not be compromised through lossy image compression during storage or transmission.
5. While 10 finger biometric and photographs can ensure de-duplication accuracy higher than 95% depending upon quality of data collection, there may be a need to improve the accuracy and also create higher confidence level in the de-duplication process. Iris biometric technology, as explained above, is an additional emerging technology for which the Committee has defined standards. It is possible to improve de-duplication accuracy by incorporating iris. Accuracy as high as 99% for iris has been achieved using Western data. However, in the absence of empirical Indian data, it is not possible for the Committee to precisely predict the improvement in the accuracy of de-duplication due to the fusion of fingerprint and iris scores. The UIDAI can consider the use of a third biometric in iris, if they feel it is required for the Unique ID project.
6. A scheme must be designed to reward enrolling agencies for the capture of good quality images.

7. Specific best practices indicated in Section 12 should be observed in order to ensure interoperability, vendor independence, conformance to standards and improved performance.
8. The UIDAI along with other stakeholders should establish center(s) for on-going biometrics research, and provide reference implementation of enrolment process software designed for Indian conditions.

2 Introduction

The UID Authority of India (UIDAI) has been setup by the Govt. of India with a mandate to issue a unique identification number to every resident in the country. The UIDAI proposes that it create a platform to first collect the identity details of residents, and subsequently perform identity authentication services that can be used by government and commercial service providers. A key requirement of the UID system is to minimize/eliminate duplicate identities in order to improve the efficacy of the service delivery.

The UIDAI has selected the biometrics feature set as the primary method to check for duplicate identity. In order to ensure that an individual is uniquely identified in an easy and cost-effective manner, it is necessary to ensure that the captured biometric information can be used to carry out de-duplication. Consequently, for government and commercial providers to authenticate the identity at the time of service delivery, it is necessary that biometric information capture and transmission are standardized across all partners and users of the UID system.

The Government of India has in the past set up a number of expert committees to establish standards for various e-governance applications in the areas of Biometrics, Personal Identification and location codification standards. These committees have worked out standards in their respective categories, which may be uniformly applied for various e-governance standards.

As the UIDAI proposes to use biometrics for de-duplication and verification/authentication, it becomes essential to review the applicability and sufficiency of these standards in UID applications. It may also be necessary to enhance or clarify these standards,, and frame the methodology for the implementation of biometrics to ensure that they serve the specific requirements of the Authority.

4 Scope

- To develop biometric standards that will ensure the interoperability of devices, systems and processes used by various agencies that communicate with the UID system.
- To review the existing standards and, if required, modify/extend/enhance them so as to serve the specific requirements of the UIDAI.
- To specify design parameters of the standards that will be used for the UID system.
- To estimate the accuracy achievable using different biometric modalities in the Indian environment.
- To make recommendations to the UIDAI on the use of biometric modalities.

From the standpoint of the biometrics industry, the UID system is a civilian application of biometrics. Although the primary focus is the UID system, the Committee believes that the specifications should meet the needs of all civilian applications. The Committee considers forensic application requirements out of scope.

3 Objective

The UIDAI biometrics committee ("the Committee") was constituted to provide the UIDAI with direction on the biometrics standards, suggest best practices and recommend biometric modalities for the UID system (Annexure I).

The objective of these biometrics specifications is to ensure consistent good quality biometric images and reliable interoperability across biometric capture devices, capture software and UID service delivery.

The success of the Unique ID is solely based on its ability to detect and eliminate duplicate identities during the enrolment process. The primary method for detecting duplicates will be through the comparison of the biometric feature set, which requires consistent, high quality images. A good biometric implementation design that ensures consistent quality from a variety of biometric capture devices is therefore, essential.

The biometrics will be captured for authentication by government departments and commercial organizations at the time of service delivery. They will invariably use capture devices and biometric software vendors different from the devices and software used by UIDAI. Consequently, biometric standards are essential to ensure reliable interoperability at reasonable cost during the authentication phase.

The purpose of this document is to identify applicable standards and recommend best practices to the UIDAI to achieve its objective.

5 Target Audience

Any person or organization involved in designing, testing or implementing UID or UID compatible systems for the central government, state government or commercial organizations.

Any vendors and integrators of biometric devices and software targeting UID system compatibility.

6 Normative Reference

The following reference documents are indispensable for the application of this document.

IAFIS-IC-0110 (V3), WSQ Gray-scale Fingerprint Image Compression Specification 1997

ISO/IEC 15444 (all parts), Information technology – JPEG 2000 image coding system

ISO/IEC 19785-1:2006. Common biometric exchange formats framework – Part 1: Data elements specifications

ISO/IEC 19794-2:2005. Biometric data interchange formats – Part 2: Finger minutiae data

ISO/IEC 19794-4:2005. Biometric data interchange formats – Part 4: Finger Image data

ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face Image data

ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris Image data

ISO/IEC CD 19794-6.3. Biometric data interchange formats – Part 6: Iris Image data working group draft

MTR 04B0000022. (Mitre Technical Report), Margaret Lepley, Profile for 1000 Fingerprint compression, Version 1.1, April 2004. Available at http://www.mitre.org/work/tech_papers/tech_papers_04/lepley_fingerprint/lepley_fingerprint.pdf

7 Standards

In the current IT world, as interoperability between devices and IT systems becomes a growing concern, the question is not whether to use standards but which standards to use. ANSI, INCITS, CEN, Oasis and ISO are just a few of the prominent agencies with published biometrics standards. After reviewing the charter of each body and current state of biometrics in India, the Committee selected the ISO standard. Within the ISO body of biometrics standards, the Committee will use data format standards. These standards are widely supported by vendors, and are used extensively. ISO data format standards also contain the maximum empirical information on usage, interoperability and conformance.

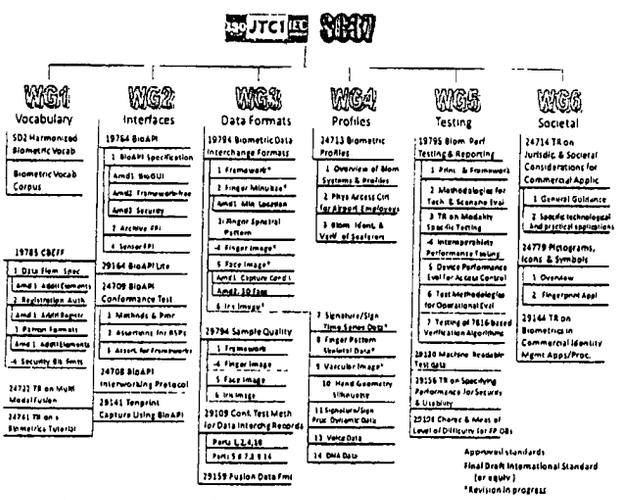


Figure 1 ISO Biometrics Standards Activity

8 Tailoring of Face Image Standards

The UIDAI Fingerprint Image Standard will adopt ISO/IEC 19794-5 Face Image Data Standard as the Indian Standard and will specify certain implementation values (tailoring) and best practices.

8.1 Section 7 Digital/Photographic requirements

The UIDAI will require face images for human visual inspection and duplicate check on a small subset. Visual inspection and automatic matching accuracy is directly related to the quality of the images. Therefore it is essential that the highest quality of images be consistently captured.

8.1.1 For Enrollment and Authentication

Defining the values for face image standards as shown in Section 7.2, table 2.

Face Image Type Code	Scan resolution (dpi)	Color Space Code	Source Type Code	Inter-eye distance (pixels)	Facial Expression Code
Full Frontal (0x01)	300	24 bit RGB (0x01)	0x02 0x06	120	0x01

8.1.2 Source Type

Static face images (Code 0x02) from a digital still-image camera are strongly recommended. Single video frames from a digital video camera (Code 0x06) are also acceptable.

16.1.3 Expression

Face images should have neutral expression (non-smiling) with both eyes open and mouth closed.

16.1.4 Pose

Roll, pitch and yaw angle should not be more than $\pm 5^0$ (Figure 4 of ISO 19794-5).

8.2 Section 7 Image Compression Algorithm

8.2.1 For Enrolment

For enrolment, uncompressed images are strongly recommended. Lossless JPEG 2000 color compression will be accepted for legacy purposes only.

16.2.2 For Authentication

Code 0x01 - JPEG 2000 compression is recommended. Maximum compression ration is 10.

8.3 Face Record Format

8.3.1 CBEFF Header

The UIDAI will not use information defined in Section 5.3 of ISO document.

8.3.2 Facial Record Header

The UIDAI will maintain single facial image.

8.3.3 Facial Information Block

The UIDAI will not use information defined in Sections 5.5.1 to 5.5.6 of ISO document.

8 3.4 Feature Point Block

The UIDAI will not use geometric feature points defined in Section 5.6 of ISO document.

9 Tailoring of Fingerprint Image Standard

The UIDAI Fingerprint Image Standard will adopt ISO/IEC 19794-4 Fingerprint Image Data Standard as Indian Standard and specify certain implementation values (tailoring) and best practices.

9.1 Section 7: Image Acquisition Requirements

The duplicate check during the enrolment phase will use 1:N matching. 1:N matching for large gallery size and high enrolment rate will require substantial computing resources. The matching time and matching accuracy is directly related to the quality of the images. Therefore it is essential that the highest quality of images be consistently captured. It is also required that all ten fingers are captured whenever physically possible.

The goal during authentication is to achieve fast overall response while permitting a wide variety of capture devices and associated software. It is sufficient to capture only one or two fingers for reliable 1:1 authentication. The image quality needs for authentication are not as stringent as in enrolment.

9.1.1 For Enrolment

Setting level 31 or higher as shown in Section 7.1, table 1

Setting level	Scan resolution (ppcm)	Scan resolution (dpi)	Pixel depth (bits)	Dynamic range (gray levels)	Certifications
31	197	500	8	200	EFTS/F

9.1.2 For Authentication

Setting level 28 or higher as shown in Section 7.1, table 2

Setting level	Scan resolution (ppcm)	Scan resolution (dpi)	Pixel depth (bits)	Dynamic range (gray levels)	Certifications
28[1]	118	300	4	12	UID
30	197	500	8	80	None

9.2 Section 8 Finger Image record Format

9.2.1 Section 8.2.14 Image compression algorithm

9.2.1.1 Enrolment

Code 0 and 1 are strongly recommended. For legacy purposes only, lossless compression of code 2, 4 and 5 will be accepted.

9.2.1.2 Authentication

Code 4, compressed – JPEG 2000 is recommended. Code 0, 1, 2 and 5 are also acceptable. Code 3 must not be used. Maximum compression ration is 15.

---

[1] Level 28 is not specified in FBI's Electronic Fingerprint Transmission Specifications, Appendix F (commonly referred to as EFTS/F). It has been created to accommodate certain class of new generation lower cost single finger capture devices.

9.2.2 Section 8.3.3 Finger/palm position

The valid values for finger/palm position are 0 through 10, 13 through 15.

9.2.3 Section 8.3.7 Impression type

For enrolment image, only code 0 or 9 will be used. Authentication impression can be of type 0, 1, 8 or 9.

9.2.4 Section 8.3.10 Finger/palm image data

The estimated optimal fingerprint image captured under aforementioned specification of this standard in bitmap is 7.5MB per subject.

10 Tailoring of Minutiae Format Standard

UID Minutiae Format Standard will adopt the ISO/IEC 19794-2 Minutiae Format Standard as the Indian Standard and specify certain implementation values (tailoring) and best practices.

10.1 Section 7.4.1.3 Impression Type

For enrolment image, only code[2] 0 or 9 will be used. Authentication impression can be of type 0, 1, 8 or 9.

10.2 Section 7.5 Extended Data

While the extended data area allows for the inclusion of proprietary data within the minutiae format, this is not indented to allow for alternate representation of data that can be represented in open manner, as defined in ISO/IEC 19794-2. In particular, ridge count data, core and delta data or zonal quality information shall not be represented in proprietary manner to the exclusion of publicly defined data formats.

The UID authentication process will not utilize extended data area for verification.

[2] Codes specified in ISO/IEC 19794-4, Section 8.3.7 are newer and superset of this table. Hence the reference is made to ISO/IEC 19794-4 Table 7.

11 Tailoring of Iris Standards

UID Iris Image Standard will adopt the ISO/IEC 19794-6 Iris Image Data Standard as the Indian Standard and specify certain implementation values (tailoring) and best practices. The current (2005) version is under revision. A new version (2010) is expected to clear the ISO/IEC JTC 1/SC 37 sub-committee in January 2010. Therefore all references below are to the latest (November 2009) draft of the proposed standard. The Committee will revise this section after the ISO standard is published.

11.1 Section 7.4.2.2 Kind

Allowable values are KIND-VGA (2) and KIND_CROPPED (3) in Table 5.

11.2 Section 7.4.2.4 Image data

Every effort must be made by the vendor to register Capture Device Vendor ID and Capture Device Type ID with the appropriate registration authority. It is strongly recommended that these fields as described in Table 6 not be filled with zero value.

It is strongly recommended that quality information consisting of Quality score, Quality algorithm vendor ID and Quality algorithm ID as described in Table 6, shall be provided.

12 Best Practices

Specific recommendations for each modality listed below are based on prevailing standards, best practices followed by international users and the ground reality in India.

12.1 Face

Key Decisions	Decision Type	Summary of Decisions
Enrolment		
Image capture	R	Full frontal, 24 bit color
Digital/Photographic requirements	R, S	Per ISO 19794-5 Section 7.3, 7.4, 8.3 and 8.4 with Section 8.3 of Technical Corrigendum 2. Inter-eye distance – minimum 120 pixels.
Pose	S	Per ISO 19794-5 Section 7.2.2
Expression	R, S	Neutral expression. Specified as best practices.
Illumination	S	Per ISO 19794-5 Section 7.2.7
Eye Glasses	S	Per ISO 19794-5 Section 7.2.11
Accessories	R	Permissible for medical and ethical reasons only.
Multiple samples of face	M	Yes. Recommended for automatic face recognition.
Operational	S	Per ISO 19794-5 Section 7.2.4 - 7.2.10
Assistance	R	Yes. Specified as best practices.
Segmentation and feature extraction	M	Recommended for automatic face recognition
Quality check	R	Yes. Specified as best practice.
Storage & compression	S	Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 color accepted.
Authentication		
Image capture	R	Same as enrollment
Compression	S	JPEG 2000 color compression recommended. Compression ratio to be less than 10:1.
Number of Images	R	One full frontal image

Figure 2 Face image

178

12.2 Fingerprint

Key Decisions	Decision Type	Summary of Decisions
Enrolment		
Image capture		
Plain or rolled	R	Plain, live scan
Number of fingers	R	Ten
Device characteristics	S	Setting level 31 or above, EFTS/F certified
Quality check	R	Yes - specified as best practice
Operational		
Assistance	R	Yes - Specified as best practice
Corrective measure	R	Yes - Specified as best practice
Storage & transmission		
Compression	S	Uncompressed images strongly recommended. For legacy reasons, lossless JPEG 2000 or WSQ compression accepted.
Storage format	S	Per ISO Section 8.3. No deviation necessary
Minutiae format	S	Per ISO 19794-2. No deviation necessary.
Multi-finger fusion algorithm	R	Recommended. Application dependent.
Authentication		
Image capture		
Number of fingers	R	No minimum, no maximum. Application dependent. Recommended as best practice
Any finger option	M	Yes. Recommended as best practice
Retry	R	Maximum 5. Recommended as best practice.
Device characteristics	S	Setting level 28 or above
Transmission format	S	Per ISO. No tailoring necessary
Compression	S	JPEG 2000 compression recommended. Compression ratio to be less than 15:1
Minutiae format	S	Per ISO 19794-2. No tailoring necessary

Figure 3 Fingerprint

[3] R: Recommendation based on best practice/empirical data, S: Standard based, M: Management judgment.

12.3 Iris

Decision		Decision Type	Summary of Decision
Enrolment			
	Image	R	Two eyes, > 140 pixel image diameter (170 pixel preferred), image margin 50% left and right, 25% top and bottom of iris diameter
	Device Characteristics	R	Tethered, autofocus, continuous image capture, exposure < 33 milli-second, distance >300 mm for operator control, > 100mm enrollee control
	Operational	M	Operator controlled strongly preferred. No direct natural or artificial light reflection in the eye, indoor.
	Segmentation	R	Non-linear segmentation algorithm
	Quality Assessment	R	Per IREX II recommendations[4]
	Compression & Storage	S	ISO 19794-6 (2010) data format standard as tailored in Section 11. JPEG 2000 or PNG lossless compression, KIND_VGA of Table A.1 of ISO 19794-6 (2010).
Authentication		R, S	Same as enrollment except One or two eyes JPEG 2000 KIND_CROPPED of Table A.1

Figure 4 Iris

12.4 Biometrics Accuracy

The UIDAI's charter of assuring uniqueness across a population of 1.2 billion people mandates the biometrics goal of minimizing the False Accept Rate (FAR) within technological and economical constraints.

All published empirical data is reported using Western populations and database sizes of tens of millions. An accuracy rate (i.e., True Acceptance Rate) of 99% is reported in the test of commercial system performance[23]. Two factors however raise uncertainty on the extent of accuracy achievable through fingerprints: First, the scaling of database size from fifty million to a billion has not been adequately analyzed. Second, the fingerprint quality, the most important variable for determining accuracy, has not been studied in depth in the Indian context.

[4] IREX II study conducted by NIST will be published in April 2010. It will provide definite empirical result of impact of image quality on matching accuracy and speed. For fingerprint the analogous study resulted in creation of NFIQ, NIST Fingerprint Image Quality algorithm. We anticipate similar outcome from IREX II. IREX II will be normative annexure to ISO 19794-6 (2010).

A technical sub-group was formed to collect Indian fingerprints and analyze quality. Over 250,000 fingerprint images from 25,000 persons were sourced from districts of Delhi, UP, Bihar and Orissa. Nearly all were from rural regions, collected by different agencies using different capture devices and through different operational processes. Analysis reported in Annexure showed the UIDAI could obtain as good fingerprint quality as seen in developed countries, provided that proper operational procedures are followed and good quality devices are used. On the other hand there is data to suggest that quality and therefore the accuracy drops precipitously if attention is not given to operational processes.

Based on rather extensive empirical results compiled by NIST and a first cut of Indian data analyzed in a short period, the following broad categorization can be made

1. The UIDAI can obtain fingerprint quality as good as that seen in developed countries. There is good evidence to suggest that fingerprint data from rural India may be as good as elsewhere when proper operational procedures are followed and good quality devices are used. There is also data to suggest that quality drops precipitously if attention is not given to operational processes.
2. It is possible to closely predict the expected fingerprint recognition performance. In the experiments, at 95% confidence, the sample database of a rural region is expected to achieve similar accuracy as Western data. By extrapolating NIST analysis of Western data, it is possible to conclude that fingerprint alone is sufficient to achieve minimum accuracy level of 95%, with moderately good fingerprints images.
3. Face is an invaluable biometric for manual verification. Its potential to contribute materially to improved FAR rate is however, limited particularly because of extremely large database size and high value of target accuracy.
4. Iris can provide accuracy comparable to fingerprint. Therefore fused score of two uncorrelated modalities will provide better accuracy than any single modality and could achieve the target accuracy.

Empirical data has highlighted several non-technical factors that can impact accuracy more significantly than technical accuracy improvement efforts.

- Simple operational quality assurance. A few simple operational techniques such as keeping a wet towel or maintaining the device in good working order can be superior to squeezing an additional fraction of a percent in accuracy rates through technical improvements. An unchecked operational process can increase the false acceptance rate to over 10%.
- In the data analyzed, 2% to 5% of subjects did not have biometric records. Missing biometrics is a license to commit fraud. It is believed that the failure is due to poorly designed processes. The enrolment process when examined, had loopholes which prevented it from detecting such omissions.
- The biometric software needs to be tuned to local data. Un-tuned software can generate additional errors in the range of 2 to 3%.

13 Members

13.1 Biometrics Committee

	Name, Affiliation
1.	Dr. B. K. Gairola, DG NIC – Chairman
2.	Dr. C. Chandramauli – Registrar General of India (RGI) – Member
3.	Dr. D. S. Gangwar, Joint Secretary, Rural Development- Member
4.	Dr. A. M. Pedgaonkar, RBI – Member
5.	Mr. Pravir Vohra, ICICI – Member
6.	Prof. Deepak Phatak, IIT Bombay – Member
7.	Prof. Phalguni Gupta, IIT Kanpur – Member
8.	Mr. R. S. Sharma, DG UIDAI – Member/Convener
9.	Mr. Rajesh Mashruwala, UIDAI – Member
10.	Mr. Srikanth Nadhamuni, UIDAI – Member

13.2 Face Sub-committee

1.	Dr. Richa Singh
2.	Dr. Mayank Vatsa
3.	Mr. Rajesh Mashruwala

13.3 Fingerprint Sub-committee

1.	Prof. Phalguni Gupta
2.	Dr. A. M. Pedgaonkar
3.	Mr. Rajesh Mashruwala
4.	Dr. Mayank Vatsa

13.4 Iris Sub-committee

1.	Prof. Phalguni Gupta
2.	Dr. Mayank Vatsa
3.	Mr. Rajesh Mashruwala

Annexure I
Notification of UIDAI constituting the Committee

183

No 45/DG-UIDAI/2009
Government of India
Planning Commission
Unique Identification Authority of India

R No.321, Yojana Bhavan
New Delhi – 110 001

Dated. September 29, 2009

OFFICE MEMORANDUM

The UID Authority of India has been setup by the Govt. of India with a mandate to issue a unique identification number to all the residents in the country. The main objective is to improve benefits service delivery, especially to the poor and marginalised sections of the society. To deliver its mandate, the UID Authority proposes to create a platform to first collect the identity details and then to perform authentication that can be used by several govt. and private service providers. A key requirement of the UID system is to minimize/eliminate duplicate UIDs in order to improve the efficacy of the service delivery. A possible way to ensure uniqueness of IDs (so that one resident gets only one ID) is to use biometric technologies. In order to ensure that an individual is uniquely identified and authenticated in an easy and cost-effective manner, it is necessary to ensure that the biometric information which is captured is capable of carrying out the de-duplication at the time of collection of information Further, in order to achieve interoperability it is important that the capture and use of biometric information is standardized across all the partners and users of the UID system.

The Government of India, in the past, had set up a number of expert committees for standards to be used for various e-governance applications in areas of Biometrics, Personal Identification and location Codification Standards These committees have worked out few standards in the respective categories to be uniformly applied for various e-governance standards.

As UIDAI proposes to use biometrics for de-duplication and verification/authentication, it becomes essential to review the applicability and sufficiency of these standards in UID applications, modify/extend/enhance them to ensure that they serve the specific requirements of UIDAI and frame the methodology for its implementation.

In view of the above, a Committee for framing the Biometric Standards for UIDAI is being setup to review the existing standards and modify/extend/enhance them so as to achieve the goals and purpose of UIDAI for de-duplications and authentication

1. Charter of the Biometric Standards Committee

- To develop biometric standards that will ensure interoperability of devices, systems and processes used by various agencies that use the UID system.
- To review the existing standards of Biometric and, if required, modify/extend/enhance them so as to serve the specific requirements of UIDAI relating to de-duplication and Authentication.

2. Composition of the Biometric Standards Committee

Following will be the composition of the Biometric Standards Committee:

1. Dr. BK Gairola, Director General, National Informatics Centre - Chairman
2. Dr. C. Chandramauli – Registrar General of India - Member
3. Dr. DS Gangwar, Jt Secretary, Min of Rural Development - Member
4. Dr. AM Padgaonkar, Reserve Bank of India – Member
5. Mr. Pravir Vora, ICICI - Member
6. Dr. Deepak Phatak, IIT Bombay - Member
7. Dr. Phalguni Gupta, IIT Kanpur – Member
8. Two Representatives from Technology Team of UIDAI – Members
9. Director General, UIDAI or his Nominee – Member/Convenor

Unique Identification Authority of India (UIDAI) will service this Committee.

The Committee will be able to invite representatives from user organisations and other Technology Experts as Special Invitees to solicit their views and advice on various aspects on the issue.

3. Technical Committee and Working Groups

The committee can also set up sub-committees that focus on various aspects of biometric standards such as fingerprints, Iris and facial image and working groups for conducting/developing reference implementations/proof-of-concept (POC) studies, specific research, field testing etc. on an as-needed basis. The Committee may meet from time to time and draft the standard document based on the feedback of sub committees and working groups and submit recommendations. The Committee may also set its own review process before recommending the final standards.

Working Groups can be created to assist the above committees by conducting proof-of-concept (POC) studies, specific research, field testing etc.

4. Review process

It is important that the standards remain unbiased, pragmatic, vendor neutral, interoperable, and cost effective. In biometrics where technology continues to progress rapidly, three parties - vendors, academia and enterprise users - have great deal of knowledge of the technology The Committee's review process will leverage their knowledge without compromising on its charter.

The technical committee will publish a draft version of the document and solicit structured feedback from the members of the committee, technology vendors, academia and enterprise users. Such review process will also provide sufficient advance notice to the vendors to begin upgrade to their solution, thus reducing lead time between the final standards adoption and conforming solutions.

The feedback from the various groups will be reviewed by the technical committee and suitable changes made in order to incorporate useful inputs. The final draft will be sent over for a final review and then the ratified version of the standards will be released

5. Deliverables of the committee

- Obtain consensus from Government stakeholders to adopt and use a common set of standards for interoperability, containment of biometrics system cost and wide spread propagation of Biometrics in governmental and private sectors.
- Review the existing standards of Biometric and, if required, modify/extend/enhance them so as to serve the specific requirements of UIDAI relating to de-duplication and Authentication.
- Ratify Biometrics standards from applicable base Indian and International standards, which meet needs of the UIDAI.
- Recommendation to UIDAI users to assure Interoperability of biometrics data
- Develop certification criteria for conformity, interoperability and performance.
- Maintain & Publish registry of recommended biometrics standards, interoperability recommendations and certification criteria

157

186

6. Time-Frame

Keeping in view the commitment of UIDAI to start issuing UIDs within twelve to eighteen months, it is necessary that the Committee presents its report on standards as early as possible. Hence the Committee will present its Final Report to the undersigned on Biometric Standards to be adopted by UIDAI within 90 days of its constitution.

7. Miscellaneous

The non-official members of the Committee and Special Invitees will be reimbursed the cost of their travel and other incidental expenses as per Rules as and when they travel to attend the Committee meetings.

29.9.09

(R S Sharma)
Director General & Mission Director

Copy forwarded to the Chairman and Members of the Committee for information and necessary action.

Copy to: Cabinet Secretary/ Principal Secretary to the PM/All Secretaries to Govt. of India/All Chief Secretaries of the States/UTs for information.

Annexure II Technical Data

Biometrics Basics

Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioural attributes of the person. The relevance of biometrics in modern society has been reinforced by the demand for large-scale identity management systems whose functionality relies on accurately determining an individual's identity. No single biometric is expected to effectively meet all the requirements imposed by all applications. In other words, no biometric is ideal, but a number of them are admissible[1].

Demographic data is used along with the biometric information to improve the de-duplication process. For example, when a duplicate is suspected, a manual review of all available information of the person will also include a review of the demographic data.

Face

Photos of the face are commonly used in various types of identification cards and there is wide public acceptance for this biometric identifier. Face recognition systems are the least intrusive type of biometric sampling system, requiring no contact or even awareness of the subject. The face biometric can work with legacy photographs, videotapes and other image sources.

A face needs to be well lighted using controlled light sources for automated face authentication systems to work well. There are many other such technical challenges associated with robust face recognition. Face is currently a poor biometric for use in de-duplication. It performs better in verification but not at the accuracy rates that are sometimes claimed. An obvious way for an undesirable person to avoid face identification is by the use of disguise, which will cause False Negatives in a screening application. In general, it is a good biometric identifier for small-scale verification applications.

Fingerprint

There is a long tradition in the use of fingerprints for identification. Fingerprints are easily sampled with low-cost fingerprint scanners. They can also be sampled by traditional low-tech means and then cheaply and easily converted into digital images. Fingerprints also lend themselves very well to forensic investigation.

There is a large variation in the quality of fingerprints within the population. The appearance of a person's fingerprint depends on age, dirt, and cuts and worn fingers, i.e., on the occupation and lifestyle of the person in general. Sampling of the fingerprint is through contact, i.e., pressing the finger against the platen of a fingerprint reader. As a result, there can be technical problems because of the contact nature of acquisition and problems related to the cleanliness of the finger and the platen. Additionally, there are people who may not have one or more fingers [5].

Fingerprint technology constitutes approximately half of the total biometrics market[5].

Iris

The iris is the annular region of the eye, bounded by the pupil and sclera on either side. Iris is widely believed to be the most accurate biometric, especially when it comes to False Accept Rates. Therefore, the iris would be a good biometric for pure de-

---

[5] IDC & Acuity Market Research Reports.

duplication applications. The iris sample acquisition is done without physical contact and without too much inconvenience to the person whose iris image is being acquired. Iris has no association with law enforcement and has not received negative press and may therefore be more readily accepted.

There are few legacy databases and not much legacy infrastructure for collection of the iris biometric. Large-scale deployment is consequently impeded by the lack of an installed base. This will make the upfront investment much higher. Since the iris is small, sampling the iris pattern requires a lot of user cooperation or the use of complex and expensive devices. The performance of iris authentication can be impaired by the use of spectacles or contact lenses. Also, some people may be missing one or both eyes while others may not have the motor control necessary to reliably enroll in an iris based system.

Until recently, iris code representation and matching was proprietary and patented. Iris is emerging as the third standard biometric identifier after expiration of patents and changes in vendor practices.

The gross false accept and false reject error rates associated with the fingerprint, face and iris modalities reported in literature are shown in Figure 5 [2].

Biometric identifier	Reference	FRR	FAR
Fingerprint	NIST FpVTE	0.1%	1%
Face	NIST FRVT	10%	1%
Voice	NIST 2004	5-10%	2-5%
Iris	ITIRT	0.99%	0.94%

Figure 5 FAR and FRR error rates

190

Face Image Best Practices

Summary

Face images will be used primarily for human visual inspection. However, automatic face recognition may be used as the secondary means of authentication/de-duplication. Figure 6 summarizes key decisions for face images.

Key Decisions	Decision Type	Summary of Decisions
Enrolment		
Image capture	R	Full frontal, 24 bit color Inter-eye distance - minimum 120 pixels.
Digital/Photographic requirements	R, S	Per ISO 19794-5 Section 7.3, 7.4, 8.3 and 8.4 with Section 8.3 of Technical Corrigendum 2.
Pose	S	Per ISO 19794-5 Section 7.2.2
Expression	R, S	Neutral expression. Specified as best practices.
Illumination	S	Per ISO 19794-5 Section 7.2.7
Eye Glasses	S	Per ISO 19794-5 Section 7.2.11
Accessories	R	Permissible for medical and ethical reasons only.
Multiple samples of face	M	Yes. Recommended for automatic face recognition.
Operational	S	Per ISO 19794-5 Section 7.2.4 - 7.2.10
Assistance	R	Yes. Specified as best practices.
Segmentation and feature extraction	M	Recommended for automatic face recognition
Quality check	R	Yes. Specified as best practice.
Storage & compression	S	Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 color accepted.
Authentication		
Image capture	R	Same as enrollment
Compression	S	JPEG 2000 color compression recommended. Compression ratio to be less than 10:1.
Number of Images	R	One full frontal image

Figure 6 Face

Enrolment

Face image capture

Full frontal face image provides sufficient information for both human visual inspection (by operator) and automatic face recognition algorithms. In order to obtain a good quality image, 24-bit color image with minimum 90 pixels of inter-eye distance is required. The Committee recommends at least 120 pixels for optimum quality. The image should contain well-focused nose to ear and chin to crown region. In special circumstances, assistance may also be provided but in no case should the face or body part (hand, arms) of the assisting person or any object appear in the photograph.

Operational

Similar to fingerprints, the single most important factor in obtaining better image quality is the operational process. While there are many qualitative factors in designing good operational processes, operator training and assistance are important for yielding good quality images. Operators will be trained to obtain the best possible face images that satisfy requirements.

Segmentation and feature extraction

Segmentation and feature extraction are only required for automatic face recognition algorithms. The algorithms for both remain proprietary.

Quality check

Image quality is one of the most important factors for both human inspection and automatic face recognition algorithms. The quality assessment algorithm should encode parameters like illumination, pose, blur, noise, resolution, inter-eye distance, image height and width, and horizontal and vertical position of the face. The quality assessment algorithm should be used at the time of enrolment to determine the quality score of the captured face image and image is stored only if it meets a certain quality threshold.

Storage and Compression

According to Figures 12 and 13 of ISO face image standards, the performance of face recognition algorithms reduce significantly if the compression factor is greater than 10. Further, as mentioned previously, these are our national assets and should be captured and stored for long-term use. For preserving the quality of image, it is strongly recommended that uncompressed images should be stored in the database.

Authentication

The authentication process consists of steps similar to enrolment.

Image Capture

Image capture for 1:1 verification should also follow standards for enrolment as defined earlier in this Section.

Compression

For verification, images with JPEG 2000 compression ration of 10 will suffice. As per ISO standards, the image size after compression should not be less than 11 KB.

Number of Images

For both manual and automatic authentication, a single full frontal face image is sufficient. The captured image should conform to the digital/photographic requirements and quality thresholds mentioned above in the enrolment section.

193

Fingerprint Best Practices

Summary

Figure 7 summarizes the key parameters for fingerprint. The Committee further classifies the decision into

1. Standards based (S): Do ISO or other standard bodies directly provide available choices?
2. Recommendation based (R): Are there studies that provide sufficient evidence for us to make an informed decision?
3. Management judgment (M): Management decision based on project context.

The remaining section has a brief explanation of each decision.

Key Decisions	Decision Type	Summary of Decisions
Enrolment		
Image capture		
Plain or rolled	R	Plain, live scan
Number of fingers	R	Ten
Device characteristics	S	Setting level 31 or above, EFTS/F certified
Quality check	R	Yes - specified as best practice. Avoid NFIQ quality 4 and 5 level fingerprints.
Operational		
Assistance	R	Yes - Specified as best practice
Corrective measure	R	Yes - Specified as best practice
Storage & transmission		
Compression	S	Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 or WSQ compression accepted.
Storage format	S	Per ISO Section 8.3. No deviation necessary
Minutiae format	S	Per ISO 19794-2. No deviation necessary.
Multi-finger fusion algorithm	R	Recommended. Application dependent.
Authentication		
Image capture		
Number of fingers	R	No minimum, no maximum. Application dependent. Recommended as best practice
Any finger option	M	Yes. Recommended as best practice
Retry	R	Maximum 5. Recommended as best practice.
Device characteristics	S	Setting level 28 or above
Transmission format	S	Per ISO. No tailoring necessary
Compression	S	JPEG 2000 compression recommended. Compression ratio to be less than 15:1
Minutiae format	S	Per ISO 19794-2. No tailoring necessary

Figure 7 Fingerprint

Enrolment

The enrolment process can be broken down into image capture ("client") and de-duplication ("server") side components. The client side captures the image, performs local processing and storage. The server side receives the image, performs quality check and finally executes the computational intensive task of duplicate checking against the gallery.

Image capture

During image capture, the factors to consider are:

1. Type of image and number of fingers to capture
2. Device used for capturing the image
3. Immediate processing including segmentation of slap, sequencing of fingers, rotational correction and quality check of image
4. Storage when the images need to be stored

Plain or rolled

The rolled image, common in forensic applications, contains twice as much information as the plain image. The plain image is easier to capture. A slap capture device can capture up to four plain fingers in one scan. The rolled image in contrast, must be captured one finger at a time. Rolled images requires operator guiding the rolling of each finger. The operation difficulty in capturing rolled image rules out its use in the UID system.

Number of fingers

In general, every additional finger increases accuracy and improves matching speed. Quality of finger image among the fingers is correlated. Still, two poor quality finger images are better than one poor quality finger image. Considering the fingerprint quality of rural workers, the Committee recommends capturing prints of all ten fingers, the maximum possible.

Device characteristics

Device characteristics cover scan resolution, pixel depth and dynamic range. A higher resolution device does not necessarily produce better images[6]. The biometrics sample captured during enrolment needs to be the best sample possible. Therefore following best practices of leading countries, the Committee recommends the use of EFTS/F certified devices that operate at level 31 or above.

Capture & quality check

Once the image has been captured, one can perform basic quality check and image improvement. The enrollee must be asked to retry enrolling if the image quality is poor. The algorithm can assign image quality score. The quality threshold score is an important decision. Images captured with a NIST Fingerprint Image Quality (NFIQ) value of 4 or 5 normally should not be used for enrolment purposes.

---

[6] It should be noted that two devices with identical scan resolution, pixel depth and dynamic range do not provide similar quality images. A number of laboratory tests have shown that a 500 dpi device from one vendor performs better than a 1000 dpi device of another vendor. Nevertheless, these attributes are the only transparent way to specify the minimum device requirements.

Operational

The single most important factor in obtaining better image quality is the operational process. While there are many qualitative factors in designing good operational processes, the following have been shown to be critical factors:

1. Operator Assistance: Operators will be trained to guide the enrollee's hand and apply pressure if necessary to obtain best possible image quality.
2. Corrective measures & retries: If the initial capture is unsatisfactory, the operator will be trained to provide corrective measures such as wiping fingers with a wet cloth or applying lotion. Only after all such measures are exhausted in five attempts, will the operator be able to override the (forced capture) quality gate.

Storage and Transmission

Once the quality check is complete, the image needs to be retained. The data format of storage should be such that other applications can access the data.

Compression

Biometric data are national assets and should be captured and stored for long-term use. To preserve the quality, the Committee strongly recommends uncompressed images. Transmission of images may be made in JPEG 2000 or WSQ lossless compression for legacy or compatibility purposes. Any form of lossy compression is not accepted. In uncompressed mode, the total storage required for the entire population is 10,000 TB.

Storage format

ISO standard prescribed format is sufficient for our needs.

De-duplication minutiae format

The minutiae representation has been standardized. However, the standardization allows vendor proprietary data fields. The trade-off is between performance and accuracy through enhanced minutiae data versus higher level of vendor dependence. Based on the accuracy and performance trade-offs reported by NIST, it is acceptable to use the proprietary format of the extractor-matcher of the vendor selected for de-duplication.

Multi-finger fusion

Different algorithms are available to obtain consolidated score [7] and [28]. The selection of the algorithm will make material difference to the overall accuracy. ISO and other bodies do not make recommendations, nor do they provide empirical study. The UIDAI will conduct its own analysis to identify the best multi-finger fusion algorithm.

Authentication

The authentication process consists of steps similar to the enrolment process, but its requirements for accuracy, performance and interoperability are different. Since the authentication process is performing 1:1 verification, the captured image may be of lower quality compared to the image captured during the enrolment process.

Image capture

196

Number of fingers

It is obvious that a fewer number of fingers should be required for verification to achieve a satisfactory accuracy target. A single finger will be sufficient to provide the minimum standard of accuracy requirements. Applications requiring higher levels of accuracy may need additional fingers.

Any finger option

The normal practice is to use one specific finger, say the index finger for verification. However, current technology could allow the person to scan any finger. This is not merely a question of convenience. Certain fingers, depending on the condition of the finger, will perform better in matching. While one cannot easily determine this a priori, any frequent user will learn it by experience. This improves subsequent user experience and could potentially improve match accuracy.

Retry

The decision on number of retries has different implications during authentication. In case of enrolment, the final decision is to take the "best possible" image. The operator can thus "force capture". In case of authentication, the operator needs to find an alternate method of authentication if fingerprint verification fails. The operator/application would not know the cause of verification failure. The failure could be because the fingerprint did not match or image capture did not produce sufficient quality image for matching. In both cases, the match score is low enough for the system to declare "no match". A timeout will be implemented in service after five attempts.

Device characteristics

Device characteristics cover scan resolution, pixel depth and dynamic range. Higher resolution does not necessarily produce better images. Considering the UIDAI's goal of making authentication ubiquitous and the availability of low cost new technology devices, the Committee has defined a new standard for the scanner used in the authentication process. It is envisioned that the UIDAI will provide certification criteria for this standard.

Transmission format

The captured image needs to be sent to the UID server for matching in real.time. Two factors will decide the format of the image to be sent. If the transmission bandwidth is low, it is prudent to send as little data as possible. On the other hand if the computing device associated with the capture device has very limited processing power, it is prudent to do minimal amount of local computation. In the first case, the transmission will contain extracted minutiae. In the second, it will contain the compressed raw image. For example, a capture device connected to a computer communicating over a mobile network could send minutiae by performing local extraction. A dedicated image capture device with built-in network connectivity is able to do little local processing and may send raw image.

The UID software will support raw image format, compressed image format as well as ISO standard minutiae format to be transmitted, in order to provide maximum flexibility during authentication. It is understood that raw or compressed image will give a higher level of accuracy.

Compression

If the raw image is to be sent, JPEG 2000 compression is recommended, WSQ compression may be acceptable for legacy purposes. A compression of up to 15 is acceptable. While uncompressed image will be accepted, it is not recommended. JPEG compression is not accepted. There is sufficient data to indicate that compression ratio of 15 does not affect verification accuracy. Compression is not relevant if minutiae data is to be sent for verification.

Minutiae format

As discussed in the previous section, the biometric sample being transmitted could be minutiae data or image. If the data is minutiae and the UID server has matcher that best pairs with the extractor used by the authenticating agency, it will use the proprietary data. If the server does not have matching matcher, it will only use "standard" minutiae data.

Iris Image Best Practices

Summary
Compared to fingerprinting, iris capture is less studied and less standardized. For example, fingerprint scanners are tested and certified per EFTS/F standard. No such equivalent iris device certification is available. It is necessary to provide greater number of parameter specifications to ensure quality iris capture.

Figure 8 summarizes key decisions for UIDAI iris design.

Decision		Decision Type	Summary of Decision
Enrolment			
	Image	R	Two eyes, > 140 pixel image diameter (170 pixel preferred), image margin 50% left and right, 25% top and bottom of iris diameter
	Device Characteristics	R	Tethered, autofocus, continuous image capture, exposure < 33 milli-second, distance >300 mm for operator control, > 100mm enrollee control
	Operational	M, R	Operator controlled strongly preferred. No direct natural or artificial light reflection in the eye, capture location: indoor.
	Quality Assessment	R	Per IREX II recommendations[7]
	Compression & Storage	S	ISO 19794-6 (2010) data format standard as tailored in Section 11. JPEG 2000 or PNG lossless compression, KIND_VGA of Table A.1 of ISO 19794-6 (2010).
Authentication		R, S	Same as enrollment except One and/or two eyes JPEG 2000 KIND_CROPPED of Table A.1

Figure 8 Iris

The remaining section has a brief explanation of each decision.

[7] IREX II study conducted by NIST will be published in April 2010. It will provide definite empirical result of impact of image quality on matching accuracy and speed. For fingerprint the analogous study resulted in creation of NFIQ, NIST Fingerprint Image Quality algorithm. IREX II will be a normative annexure to ISO 19794-6 (2010).

Iris image

Capture of two eyes simultaneously provides several advantages[8]. Iris pattern of each eye is not correlated, giving two independent biometric feature sets. It assures correct assignment of left and right eyes and allows for more accurate estimation of roll angle.

In order to obtain good quality template, the iris image diameter should be minimum 140 native pixels. The Committee recommends 170 pixels for optimum quality.

In order to retain sufficient image surrounding of the iris for the purpose of identifying the left or right eye as well as for a more accurate iris segmentation, the margins around the iris portion of the image need to be at least 50% of the iris diameter on the left and right sides of the image, and a least 25% of the iris diameter on the top and bottom of the image.

Device Characteristics

In the typical enrolment setup, a computer will be connected to the biometrics devices to constitute the enrolment station. A tethered biometrics device provides several advantages over a stand-alone device. First, it allows the images to be associated with the enrollee demographic data at the point of capture, thus reducing possible errors. In villages where a power source may be difficult to obtain, it is simpler to supply power from the computer.

Iris capture is a new experience for the public[34]. It is faster and simpler for the operator to adjust the camera instead of the enrollee positioning himself/herself at the right distance or in the right posture. It is recommended that the capture device should be more than 300 mm away from the enrollee to be considered non-intrusive. The capture device should use auto focus and auto-capture functions. In special circumstances where the enrollee has to position himself or herself, the capture device should be more than 100mm away but the device should use a visor or other mechanical alignment aid to enable the enrollee to position themselves.

In order to provide an acceptable level of usability and ease of alignment, the camera must allow for some variability in the position of the iris center relative to the camera. This variability is defined by position tolerances in the horizontal, vertical, and axial dimensions that together define a volume (the "capture volume") within which the center of the iris must be located in order to enable image capture. For two eye capture devices, the capture volume dimensions for devices without mechanical alignment aids are 19 mm wide, 14 mm high, and 20 mm deep, and for devices with such aids, 19 mm wide, 14 mm high, and 12 mm deep.

The ability of an iris image capture device to suppress motion blur and to freeze motion, is a function of exposure time. The maximum allowable value for the exposure time is less than 33 ms, recommended being 15ms.

The iris image capture device must be capable of capturing light in the range of 700 to 900 nanometers. The camera's near infrared illuminator(s) must have a controlled spectral content, such that the overall spectral imaging sensitivity, including the sensor characteristics, transfers at least 35% of the power per any 100 nm-wide sub-band of the 700 to 900 nm range.

---

[8] Material derived from [32]

200

The iris image capture sensor shall use progressive scanning.

In order to achieve acceptable time-to-capture and FTA rates, the iris image sampling frequency must be at least 5 frames per second.

The capture devices typically provide infrared lighting using LEDs to illuminate the iris. The illumination is in a range partly visible to the human eye. Illumination shall be compliant with illumination standard IEC 825-1 and safety specification ISO 60825-1.

In order to achieve acceptable recognition accuracy, the iris acquisition sensor must achieve a signal-to-noise ration of at least 36dB.

Within the frequency range of interest, 700 to 900 nm, the iris sensor shall generate images with at least 8 bits per pixel.

Operational considerations

As mentioned earlier, it is strongly recommended that the operator and not the enrollee handle the capture device. The enrollee will be required to sit (or stand) in a fixed position, like taking a portrait photograph; the operator will adjust the camera.

The iris capture device or the connected computer shall be able to measure the iris image quality. The best practice recommendation is that an initial image quality assessment should be done to provide feedback to the operator during the capture process. The device should alert the operator if the captured iris image is of insufficient quality.

The iris capture process is sensitive to ambient light. No direct or artificial light should directly reflect off enrollee's eyes.

Segmentation and feature extraction

Segmentation and feature extraction remain proprietary. As reported in the IREX study, the vendor providing segmentation does not have to be the vendor providing matching algorithm. In fact, best of breed selection appear to be superior to any single-vendor solution.

Quality assessment

It has been noted that image quality is the single most important factor for match accuracy. IREX II study is underway to quantify and provide best practices recommendations on the image quality. The report, expected in April 2010, will become the normative annexure to ISO 19794-6 (2010). Therefore the Committee will defer detailed quality recommendations until publication of the standard.
One method widely used for ensuring good iris images is recommended here. An Iris camera takes streaming images. It is recommended that the device take successive 3 to 7 images and use local matching algorithm to match them against each other (after feature extraction). The image is considered to be of satisfactory quality if hamming distance of the match is below 0.1.

Compression and storage

The iris images, like fingerprints are considered to be national assets. They should be stored in ISO standard format using either JPEG 2000 or PNG lossless compression (KIND_VGA). It is expected that each enrollee will require 150 Kbytes of storage space, thus requiring total storage space of 200 Terabytes for the entire population.

Authentication

For 1:1 verification, any one eye will suffice, though application may require higher-level assurance whereby both eyes can be verified. Iris verification requires the image to be sent to the server for matching. It is recommended that the image be compressed to KIND_CROPPED_AND_MASKED or KIND_CROPPED using JPEG 2000. Resulting image size will between 2KB to 10 KB. Any of the larger formats specified by the ISO standard are acceptable, though not necessary.

Biometrics Accuracy

The consequences of FAR and FRR during authentication are central to the judicial design of the UID system. FAR determines potential number of duplicates, FRR determines number of enrolments necessitating manual check, hence labor cost. While trade-off between the two rates is certainly possible, there are upper bound requirements for each. Upper bound for each rate is set at 1%.

No empirical study is available to estimate the accuracy achievable for fingerprint under Indian conditions. Indian conditions are unique in two ways:

- Larger percentage of population is employed in manual labor, which normally produces poorer biometric samples.
- Biometric capture process in rural and mobile environment is less controllable compared to the environmental conditions in which Western data is collected.

To estimate achievable accuracy under Indian conditions, following methodology was employed:

1. Estimate achievable accuracy under Western conditions for a one billion sized database.
2. Estimate difference in image quality between Western and Indian conditions.
3. Using image quality, estimate change in achievable accuracy under Indian conditions.

There is no indication to believe that iris accuracy changes from one racial/geographical population to another. However, no definitive study is available.

Step 1: Estimating achievable accuracy

NIST reports FAR of 0.07% at FRR 4.4% for 6 million fingerprint gallery size using two plain fingers [21]. Similar results were reported for FBI's IAFIS System of 46M samples. It is safe to conclude that 99% accuracy (TAR) can be achieved for database size of 50 million.

	Thresholds 1300, 1880		Thresholds 1400, 2025		
Shape Filter	FAR	TAR	FAR	TAR	Matches per Second
Off	0.30%	96.3%	0.07%	95.6%	734K
On	0.32%	96.1%	0.07%	95.5%	1035K

Figure 9 Two-finger identification accuracy

Several NIST reports allow us to estimate the scaling of above data for larger gallery size and for ten fingers.

- False Acceptance Rate is linearly proportional to gallery size at constant TAR as shown in Figure 11.
- False Rejection Rate does not vary over gallery size as shown in Figure 12.
- Based on these findings, one can expect that on a database size that is 200 times larger (1.2 billion versus 6 million), the same system will have an FAR of

approximately 0.07*200 = 14%. The FRR can be expected to be about 4% based on matching of 2 finger plain fingerprints.

- Figure 10 lists effect on FAR by increasing the number of fingers for the same FRR [22].

Number of Fingers	FRR %	FAR %
2	10.3	29.2
10	10.9	0.0

Figure 10 Accuracy of multiple fingers

- Based on the above and reviewing underlying data, one can ballpark a 1,000 improvement in FAR between two-finger matching and ten-finger matching (all other things being equal). So the estimated FAR estimate of 14% should be expected to be 1,000 times less, that is, to 0.14% at FRR rate of 4%. Using further conversation factor of 10X change in FAR results in 2X change in FRR, this number is the equivalent of *FAR 1.4% at FRR rate of 2%.* In other words, NIST data indicates de-duplication accuracy (TAR) greater than 95% is achievable for ten-finger matching against a database size of one billion.

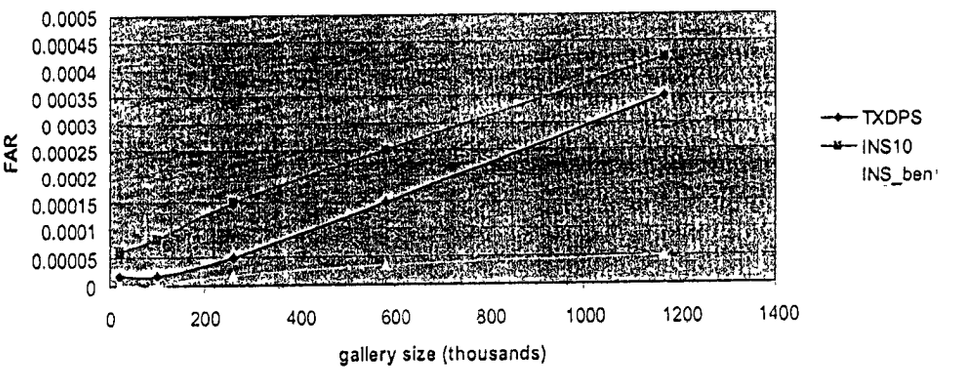


Figure 11 FAR as function of gallery size

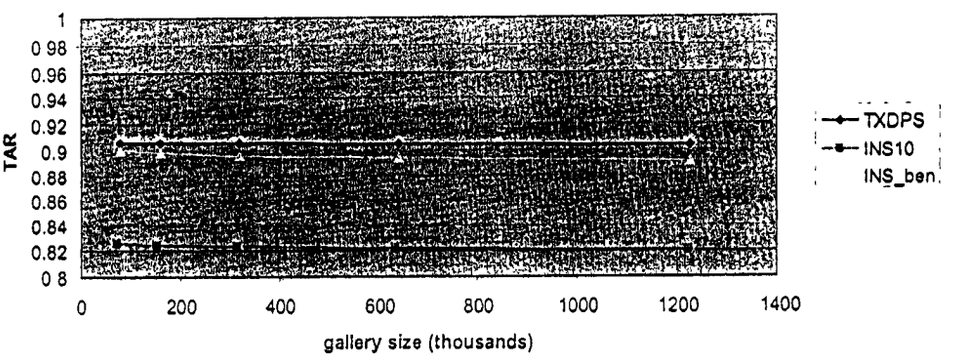


Figure 12 TAR as function of gallery size

Step 2: Image quality difference

It has been shown that match rates accuracy can be estimated from the fingerprint image quality score. NIST classifies scores into five bins. Western data accuracy rates for the bins are shown in Figure 13. Bins 1 and 2 are nearly identical, producing close to 99% true match in 1:1 verification. Bins 4 and 5 result in unacceptably low true match rates. Of particular note is bin 5, which could result in as low as 80% match rate (or 20% false accept rate).

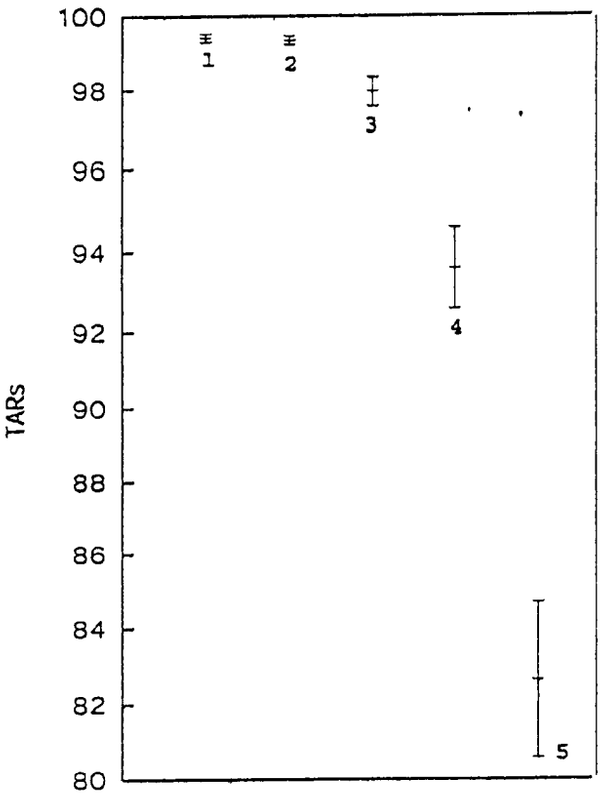


Figure 13 Accuracy Range by image quality

In a "typical" sample analyzed to arrive at the above rate[24], NIST has bin distribution shown in Figure 14 and Figure 15. Bins 4 and 5 in both datasets are less than 5% of the total sample.

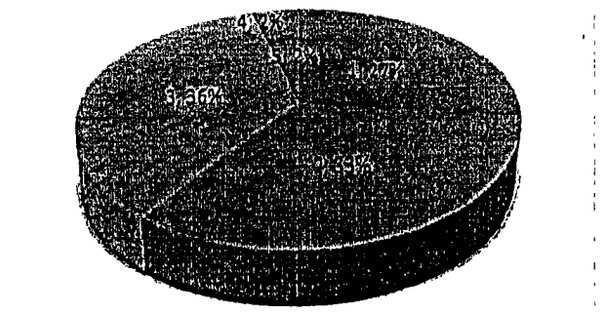


Figure 14 US-VISIT image quality distribution for right index finger

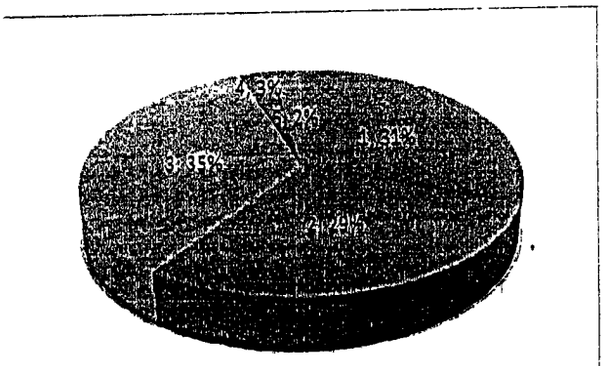


Figure 15 US-VISIT image quality distribution for left index finger

Indian Ground Conditions

The research team at IIIT Delhi focused on the ability to leverage image quality assessment tools in (1) analyzing the input biometric samples that are obtained from diverse, disparate sensors and (2) characterizing the samples based on the quality and amount of information present. Using three fingerprint databases, fingerprint image quality based experimental evaluation was performed.

1. DB1. This database contains images from 27 urban individuals (or 1350 images) and 81 rural individuals (or 1620 images). Th.s database is prepared using single impression sensor meeting FIPS 201 APL and FBI Image Quality Specifications.
2. DB2. Images captured using slap scanner. This database contains slap images from over 20,000 individuals. Each slap fingerprint image was segmented using a commercial segmentation tool. After segmentation, the database contained 200K images. The four-finger slap sensor was EFTS/F certified and operated at level 31.
3. DB3. Pre-segmented rural slap database pertaining to about 5600 individuals (around 56,000 images). The four-finger slap sensor was EFTS/F certified and operated at level 31.

Using DB1, experimental test bed and statistical tests were prepared, followed by evaluation using DB2 and DB3. Using NIST provided Fingerprint Image Quality software (NFIQ), images were classified in to bins according to the image quality score. The bin

distributions for Indian databases are shown in Figure 16 through Figure 19. Of particular interest is significantly large bin 4 & 5 numbers for DB2 as well as DB1 rural sample. In contract, DB3, another rural area shows exceptionally high bins 1 and 2.

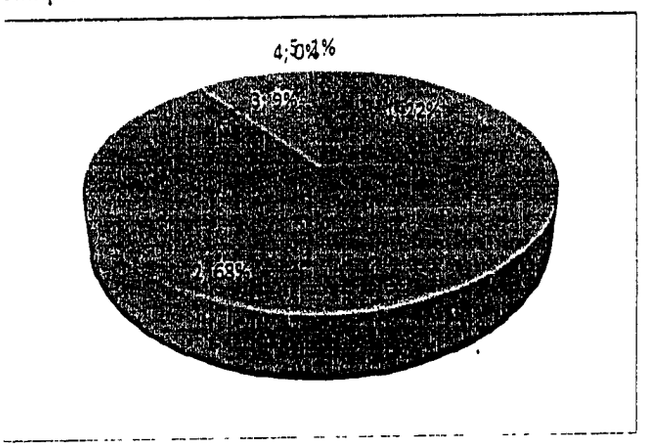


Figure 16 Image quality score distribution for DB1 Urban sample

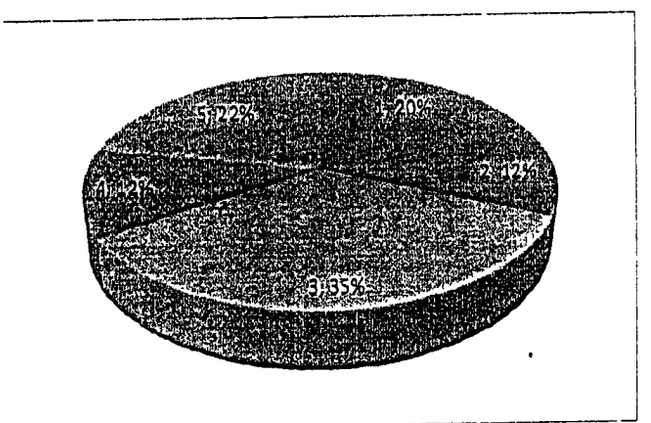


Figure 17 Image quality score distribution for DB1 Rural sample

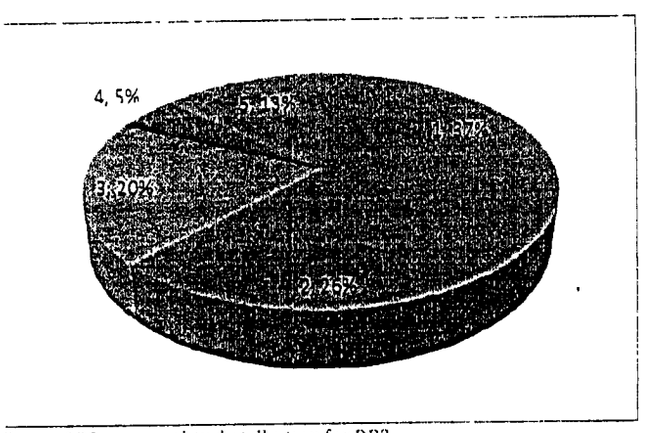


Figure 18 Image quality distribution for DB2

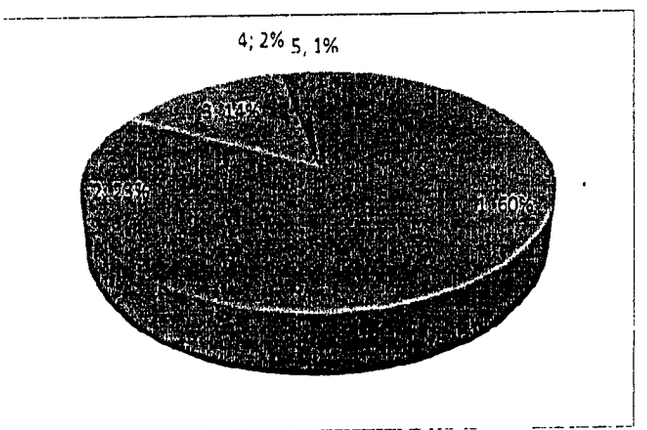


Figure 19 Image quality distribution for DB3

Step 3 Comparison & quality estimates

Since, DB2 and DB3 databases have only a single impression per finger, it is impossible to compute ROC or CMC plots and compute recognition accuracies. However, using existing Western results[24], it is possible to closely predict the expected fingerprint recognition performance.

Figure 20 and Figure 22 compare quality of left and right index finger respectively. Against x axis of accuracy (FAR), it shows cumulative bin score. Line over the Western curve (blue line) indicates that expected accuracy of the sample will be better than that of the Western population. Any points below the Western curve indicate that expected accuracy of that sample will be worse than the Western population.

DB3 shows quality superior to Western image quality while DB2 shows significantly inferior quality. While both samples are from two different rural areas of two different states, the expected accuracy is vastly different.

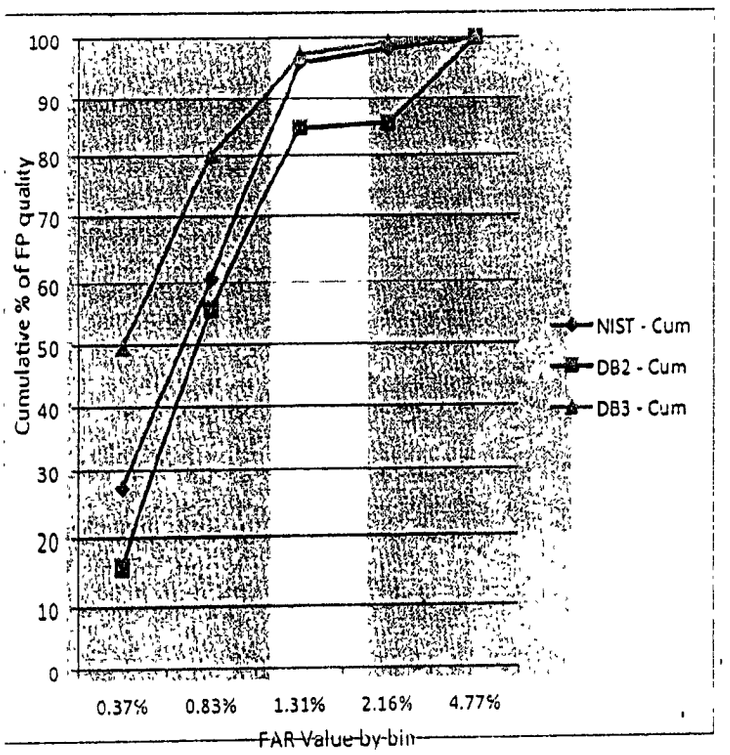


Figure 20 Right index finger comparison

Source	Bin 1	Bin 2	Bin 3	Bin 4	Bin 5
	0.37%	0.83%	1.31%	2.16%	4.77%
NIST	27.28	33.32	35.37	2.23	1.8
NIST - Cum	27.28	60.6	95.97	98.2	100
DB2	15.87	40.08	28.88	0.99	14.18
DB2 - Cum	15.87	55.95	84.83	85.82	100.00
DB3	49.73	30.51	16.97	2	0.79
DB3 - Cum	49.73	80.24	97.21	99.21	100.00

Figure 21 Right index finger numerical data

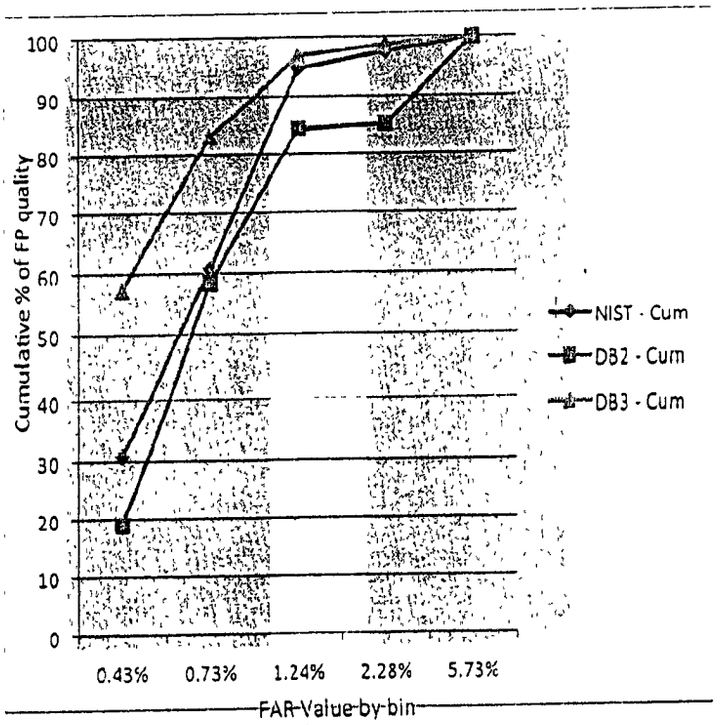


Figure 22 Left index finger comparison

Source	Bin 1	Bin 2	Bin 3	Bin 4	Bin 5
	0.43%	0.73%	1.24%	2.28%	5.73%
NIST	30.83	29.78	34.08	2.88	2.43
NIST - Cum	30.83	60.61	94.69	97.57	100
DB2	18.99	39.36	25.87	0.90	14.88
DB2 - Cum	18.99	58.35	84.22	85.12	100.00
DB3	57.25	25.77	13.8	1.87	1.31
DB3 - Cum	57.25	83.02	96.82	98.69	100.00

Figure 23 Left index finger comparison

Conclusions

NFIQ results on the databases seem to be encouraging especially if the fingerprint images are captured using good operational processes. For the majority of images, quality scores vary from excellent to good. Using these images, the typical performance of fingerprint feature extraction and matching should meet expectations. Therefore, to achieve good recognition accuracy, good quality images should be collected using optimized operational mechanisms and good sensors.

- The UIDAI can achieve fingerprint accuracy of a quality similar to developed countries. There is good evidence to suggest that Indian rural data may be as good as developed country settings when proper operational procedures are followed and good quality devices are used.
- It is possible to closely predict the expected fingerprint recognition performance. In the experiments, it is observed that, at 95% confidence, DB2 is expected to show lower accuracy compared to the Western data whereas DB3 is expected to achieve similar accuracy (for Q = 1, 2, and 3, 99% TAR with about 1% FAR).

- It is believed that DB3's improved image quality is due to better operational procedures. A few simple methods were used in DB3 data collection, such as:
  1. Using wet towels to remove dirt and moisten dry fingers
  2. Using minimum quality threshold to ensure that extra efforts are made to capture good prints from hard to obtain fingers and
  3. Keeping scanning devices in operational order

  These resulted in exceptionally good bin 1 and 2 distribution.
- It is also observed that the slap fingerprint segmentation tools require some prior training for Indian databases. After some training, segmentation results improve by 2-3%. This also suggests that in deploying a biometrics (fingerprint) system, a carefully designed a priori training set and procedure will help in improving performance.
- Since NFIQ tool is trained using Western data, there are around 4-5% errors in correctly assigning the quality scores in the Indian fingerprints. It might be possible to tune the tool to Indian data.
- When the fingerprint images in DB1 (rural and urban setting), specifically those causing errors were analyzed, it was found that there are some specific causes that are more relevant in the Indian sub-continental region compared to Western and European countries. Lawsonia Inermis (commonly known as henna or mehandi) can cause significant differences in the quality of fingerprint images. Widely used by women in the Indian sub-continent during festivals, henna is applied on hand/fingers and when applied, fingerprint sensors may not properly capture fingerprint features.
- On analyzing the quality distribution of each finger in every age group, it is difficult to generalize little fingers as useful or not. Similarly, it is not possible to generalize that, a particular age group or gender conforms to lower or higher quality scores and hence better/worse performance.

Finally, it is strongly recommended that carefully designed experiments and proper statistical analysis under pilot should be carried out, to formally predict the accuracy of biometric systems for Indian rural and urban environments.

Face identification

Face image, uncorrelated to fingerprint image, can be utilized in two ways. Face image can be independently matched using automatic matching algorithm and the results fused together to achieve higher net accuracy. NIST reports improved accuracy using fingerprint and face image score fusion [28]. It should be noted that face image alone provides low accuracy rate. A more practical method is hierarchical matching where false match rate can be improved by comparing face images of suspected duplicates obtained in fingerprint matching. In the former, the entire database has to be used as gallery, making the matching prohibitively expensive. In the later, gallery size is small, typically 1% of database. The hierarchical method improves FRR (which reduces manual duplicate check) but does not directly improve FAR (which results in duplicates in the database). However, one can trade off FRR to improve FAR.

Iris

Iris has been shown to provide accuracy comparable to fingerprint. NIST Iris test provided accuracy rates shown in Figure 24[10]. T. Mansfield of National Physical Laboratory [33] reports low FAR for small sample.

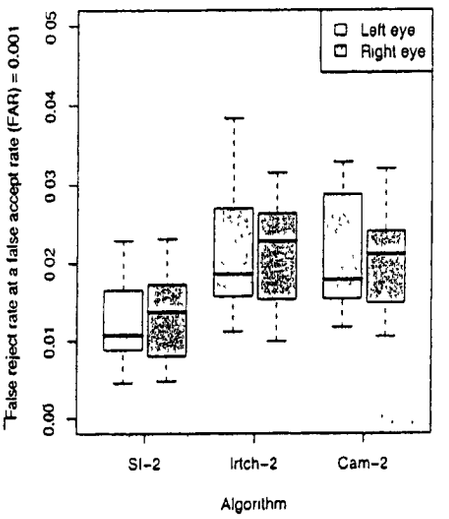


Figure 24 Iris FAR & FRR rate

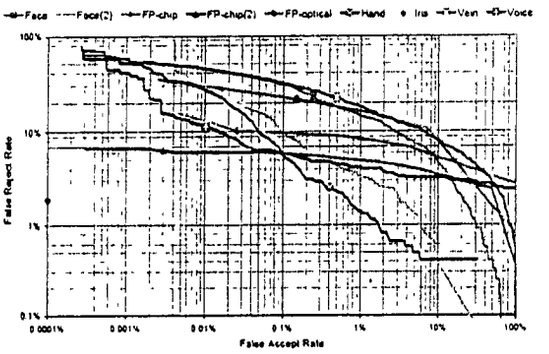


Figure 25 FAR and FRR of various biometric identifier

Fused Accuracy

A large body of literature documents the benefits of information fusion in a variety of fields including search, data mining, pattern recognition, and computer vision. Fusion in biometric is an instance of information fusion. A strong theoretical base as well as numerous empirical studies has been documented that support the advantages of fusion in biometric systems [1]. The main advantage of fusion in the context of biometrics is an improvement in the overall matching accuracy. Depending on the fusion method, the matching speed may also be improved significantly. Dr. Phalguni Gupta and his team report a study of fusion of fingerprint with iris [7]. They show a substantial improvement in matching accuracy by combining one iris with one finger. There is no empirical data available for Indian conditions though there is strong theoretical evidence that among all economically and technically feasible biometrics modalities,

combined fingerprint and iris has potential to provide maximum accuracy in Indian conditions.

213

ISO Documents

Included by reference

ISO/IEC 19794-2:2005. Biometric data interchange formats – Part 2: Finger minutiae data

ISO/IEC 19794-4:2005. Biometric data interchange formats – Part 4: Finger Image data

ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face Image data

ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris Image data

References

1. A. A. Ross, K. Nandakumar, A. K. Jain, Handbook of Multibiometrics, Springer, 2006
2. Anil Jain, Patrick Flynn, Arun Ross. Handbook of Biometrics, 2008
3. ANSI/NIST-ITL 1-2007. American National Standard for Information Systems—Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1
4. ANSI/NIST-ITL 2-2008. American Nat.onal Standard for Information Systems—Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 2 XML Version
5. Bolle, Connell et al. Guide to Biometrics, 2004
6. Fingerprint Image Data Standards for Indian e-Governance Applications, Draft Version 0.4, National Information Center
7. H. Mahrotra, A. Rattani, P. Gupta, "Fusion of Iris and Fingerprint Biometric for Recognition", Proceedings of International Conference on Signal and Image Processing (ICSIP 2006), Karnataka, India, 2006
8. IAFIS-IC-0100 (V7) Electronic Fingerprint Transmission Standard (EFTS) 1999
9. International Biometrics Group, "Independent Testing of Iris Recognition Technology, Final Report, May 2005", NBCHC030114/0002. Study commissioned by the US Department of Homeland Security.
10. IREX I, "Performance of Iris Recognition Algorithms on Standard Images", NIST Interagency Report 7629
11. ISO/IEC 19784-1:2006. Biometric Application Programming interface – Part1: BioAPI specification.
12. ISO/IEC 19794-1:2006. Biometric data interchange formats – Part 1: Framework
13. ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face image data
14. ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris image data
15. J. Cambier, "Iridian Large Database Performance", Iridian Technical Report 03-002
16. J. Daugman, "Algorithms, Performance & Challenges", BYSM, 2006
17. J. Daugman, "Iris recognition border crossing system in the UAE", International Airport Review (2) 2004.
18. J. Daugman, Technical Report 635, University of Cambridge, 2005
19. James Matey, "Iris Recognition", Sarnoff Corporation, BCC 2005
20. Jonathon Phillips, "ICE 2006 Large-Scale Results", NIST 7208, NIST, 2007
21. NISTIR 7110. Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints. C. L. Wilson, M. D. Garris, & C. I. Watson, May 2004
22. NISTIR 7112. Studies of Plain-to-Rolled Fingerprint Matching Using the NIST Algorithmic Test Bed (ATB). Stephen S. Wood & Charles L. Wilson, April 2004
23. NISTIR 7123. Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report, Charles Wilson etc al.
24. NISTIR 7151. August 2004 Fingerprint Image Quality
25. NISTIR 7201. Effect of Image Size and Compression on One-to-One Fingerprint Matching. C. I. Watson & C. L. Wilson. February 2005

26. NISTIR 7249. Two Finger Matching With Vendor SDK Matchers. C. Watson, C. Wilson, M. Indovina & B. Cochran. July 2005
27. NISTIR 7296. MINEX. Performance and Interoperability of the INCI TS 3 7 8 Fingerprint Template. Patrick Grother, Michael McCabe et al. March 2006
28. NISTIR 7346 TR. Studies of Biometric Fusion, 2007
29. Patrick Grother, Elham Tabassi, "Performance of Biometric Quality Measures", IEEE transactions on pattern analysis and machine intelligence, Vol. 29, No. 4, April 2007.
30. Registry of USG Recommended Biometric Standards, Version 2.0, NSTC
31. Report of the working group on standards for raw images of fingerprints, Reserve Bank of India
32. Shahram Orandi, Mobile ID Device Best Practice Recommendations, NIST Special Publication 500-280, August 2009
33. T. Mansfield, G. Kelly, D. Chandler, J. Kane, "Biometric Product Testing Final Report", CESG Contract X92A/4009309, Centre for Mathematics & Scientific Computing, National Physical Laboratory, Queen's Road, Teddington, Middlesex TW11 0LW
34. UK Passport Service, Biometrics Enrolment Trial, May 2005

UIDAI

Unique Identification Authority of India
Planning Commission, Govt. of India (GoI),
3rd Floor, Tower II,
Jeevan Bharati Building,
Connaught Circus,
New Delhi 110001

~~687~~

216

UID Enrolment Proof-of-Concept Report

Table of Contents

Introduction

The UID Authority of India conducted a Proof-of-Concept (PoC) study of biometric enrolment from March 2010 to June 2010 in the predominantly rural areas of Andhra Pradesh, Karnataka, and Bihar. The UIDAI also carried out the biometric enrolment of school children in the vicinity of Bangalore. About seventy five thousand people in all were enrolled during the first phase of the PoC study, and sixty thousand of the same people were re-enrolled during the second phase after a gap of three weeks.

Prior to conducting the UIDAI PoC, there was insufficient reliable biometric data available for residents of India that could be used to analyze and reach conclusions relevant to the implementation of the UID program. In addition, outside the state of Andhra Pradesh, there was no significant history of collecting iris images. In the last five years, iris image capture devices have gone through significant technological advances. There was however, limited data available from anywhere in the world regarding the ease of iris capture, as well as the usability of iris images in the case of minors. Therefore, the UIDAI felt it necessary to conduct Proof-of-Concept studies for biometric enrolment in several states, and analyze the data.

This report chronicles these Postludes. The report consists of a narrative of the activities, observations and conclusions based on numerous visits to the enrolment sites, and conclusions inferred through i) the statistical analysis of the processes and ii)by biometric analysis of the data collected during the studies.

In the study, face photos, iris images, and fingerprints of all ten fingers were captured. The ten fingerprints were captured in two different ways: first using a slap device, and then using a single finger device. Rural areas were emphasized in the study for two reasons. One was the uneven quality of fingerprints expected from rural workers whose fingerprints could be worn out by prolonged physical labour. The second was to test the UIDAI's ability to carry out biometric enrolment in locations representative of the majority of India's infrastructure, i.e. in areas with limited access to electrical power, proper lighting, and other support systems.

Objectives

The enrolment PoC was conducted to evaluate technical, operational, and behavioural hypotheses related to both the use of biometric devices and the overall enrolment process itself. It was also conducted to establish a baseline for the quality of biometric data that could be collected in rural India.

Technical objectives

i) Measure the biometric quality that could be achieved in rural Indian conditions

ii) Understand the difficulty challenges in capturing iris images,

iii) Determine suitable ergonomics in the use of the biometric devices, and understand the optimal overall layout of the enrolment station.

Operational objectives

i) Carry out a time and motion study through observation, as well as analysis of process data collected through the client software.

Behavioural objectives

i) Understand how people in rural India would respond to the capture of iris images. This was an important goal, since data on the experience of the public with iris capture devices is limited, compared to studies on fingerprint capture.

ii) Overall response of enrolees to the entire biometric capture process in the PoC needed to be understood

There were also more intangible lessons that would be directly applicable to the actual UID enrolment, since the PoC was designed to mimic UID enrolment. For instance, it was expected that the PoC experience would enable the UID team to tailor biometric enrolment best practices to be more applicable in Indian conditions.

Executive summary of outcome

1. The PoC successfully conducted over 135,000 biometric enrolments. The relative ease of conducting the operation confirmed that biometric enrolment conforming to UID standards of quality and process was indeed possible on a large scale in rural India. The total biometric enrolment time for each individual, on average, was a little over three minutes. Of this, iris enrolment took a little under a minute, and was not perceived to be excessively difficult either by the resident or the enrolling operator. Specifically, many blind people had their iris images captured (For details, see table Page 19)

2. Multiple fingerprint scanners as well as iris capture devices were used in the PoC, and they performed according to expectations. The PoC was dispersed geographically and included many rural, often remote locations across three states. The enrolment was typically conducted with minimal infrastructure and sometimes in extreme weather conditions. Enrolees varied in age all the way from four years to about ninety years of age.

3. Older people took longer to enrol than younger people, and enrolees whose employment involved manual work took longer to enrol than the rest of the PoC population. Older people needed more assistance from operators to capture of their

biometrics. However, the range of enrolment times observed was well within expectations and was not seen as making enrolment impractical.

4. The enrolment variations tested in the process led to the conclusion that the best process was one where the enrolee remained stationary during enrolment and the operator did the positioning of the devices.

5. The enrolment of children in the school showed that children in the age range of four to fifteen could be biometrically enrolled using the same process as that used for adults and with no additional difficulty. The match analysis also showed that their iris images and fingerprints could be deduplicated as accurately as those of adults.

6. The quality of the biometric capture was sensitive to the setup of the enrolment station and the process itself. Most importantly, the enrolment operator's instructions made a significant difference in the efficiency of the biometric capture.

7. The quality check process built into the enrolment software was very important and provided helpful feedback to the operator in capturing high quality images.

8. The biometric matching analysis of 40,000 people showed that the accuracy levels achieved using both iris and ten fingerprints were more than an order of magnitude better compared to using either of the two individually. The multi-modal enrolment was adequate to carry out deduplication on a much larger scale, with reasonable expectations of extending it to all residents of India.

Chronology of planning and execution

It was decided that the PoC would be done in three states: Andhra Pradesh, Karnataka, and Bihar. At least 20,000 sets of biometric data had to be collected in each state. To analyze the accuracy of biometric matching, the same set of biometric samples had to be collected again after a suitable time lag of three weeks. In order to ensure that the 20,000 sets of duplicate data could be collected, the initial enrolment target in each state was 25,000. This would allow for a minority of people not showing up for re-enrolment during the second round.

The regional offices of the UIDAI in conjunction with the technology team worked with the state governments to plan the PoC. In Andhra Pradesh and Karnataka, the Food &Civil Supplies department was designated the nodal agency for the PoC study. In Bihar, the PoC was done in conjunction with enrolment for the NREGS e-Shakti project.

Choice of locations

The following factors were considered while choosing locations for the PoC:

i) The enrolees at the PoC locations had to be representative of the Indian population in biometric quality. This meant that over eighty percent of the PoC locations

were rural, since the majority of India lives in villages. However, the remaining twenty percent of the PoC sites were urban locations close to large cities, in order to have urban areas well represented in the biometric samples collected.

ii) A further consideration was that the rural locations should be at least fifty kilometres away from the large metropolitan areas, such as Bangalore or Hyderabad. This was done since a sampling of closer locations showed that the working population of the villages close to metropolitan areas typically commuted to urban locations for work, and in general, the population was more representative of urban populations.

iii) The goal of the PoC was to collect data representative of India and not necessarily to find difficult-to-use biometrics. Therefore, extremely remote rural areas, often with populations specializing in certain types of work (tea plantation workers, areca nut growers, etc.) were not chosen. This ensured that degradation of biometrics characteristic of such narrow groups was not overrepresented in the sample data collected.

iv) For the three PoCs (apart from the school PoC), the goal was to enrol adults. In Karnataka and Bihar, only residents above 18 years were allowed to enrol. In Andhra Pradesh, adults were encouraged to enrol and very few minors actually enrolled.

The state nodal agencies in collaboration with the UID team and the enrolment agencies accordingly selected a set of locations to conduct the PoC. In Andhra Pradesh and Karnataka, two districts each were chosen for the PoC. In each district, five villages were selected for enrolling people. In Bihar, the villages scheduled for PoC enrolment was decided by the e-Shakti schedule.

The PoC was subsequently conducted in ten villages each in Karnataka and Andhra Pradesh, and in over thirty villages in Bihar. The choice of villages across states met our goal of geographic diversity since the PoC locations were widely dispersed

Within each village, the enrolment location selected was usually the local primary school or other public building (photos below). The enrolment agency brought computers, biometric devices and related equipment. In most areas, one or two power generators were also brought to provide reliable power for lighting and computers. The enrolment was carried out using locally available furniture.

PoC enrolment was also conducted in the Deputy Commissioners' offices in Mysore and Tumkur cities. Finally, PoC enrolment for school children between 4 years and 15 years was conducted in a Bangalore school. In Karnataka, the villages chosen were those with Gram Panchayat offices, i.e., larger villages. In Andhra Pradesh and in Bihar, this was not always so. The following is the list of PoC locations.

Bihar		
Gram Panchayat	Revenue Villages	Block
Bind	Bind (ward no 4 - 14), Bind (Kusar, Bishunpurand & Nirachak)	Bind
Jahana	Jahana, Chatarpur, Rampur, Nirpur, Khalsa, & Nigraian	Bind
Jamsari	Barhog, Jamsari, & Dariapur	Bind
Katrahi	Katrahi, Jakki, Bakra, Makanpur, & Makanpur (Dhullahpur)	Bind
Lodipur	Lodipur, Jaitipur, Gajipur, Ibrahimpur	Bind
Onda	Onda	Asthawan
Tajnipur	Tajnipur, Mahmudabad, Madanchak, Rasalpur, Nauranga, & Rajopur	Bind
Utarthu	Utarthu, Masia, Ahiachak, Muftipur	Bind

Andhra Pradesh		
District	Mandal	Village
Medak	Tupran	Ghanpur
	Wargal	Wargal
	Wargal	Veluru
	Chegunta	Narsingi
	Patancheru	Ward-11
Krishna	Mylavaram	Velvadam
	Kruthivennu	Lakshmipuram
	Vijayawada Rural	Nidamanuru
	Penamaluru	Poranki
	(Urban)	Vijayawada Urban Ward 9

Karnataka		
District	Taluk	Gram Panchayath or DC Office
Tumkur	Tumkur	DC Office Staff
	Tumkur	Bellavi
	Gubbi	Chelur
	Madhugiri	Dodderi
	Tiptur	Kibbanahalli
	Sira	Bukkapatna
Mysore	Mysore	DC Office Staff
	Mysore	Varuna

	HD Kote	Hommaragalli
	Nanjangud	Hadinaaru
	Hunsur	Gowdagere
	KR Nagar	Tippuru
Bangalore	School (children PoC)	Poorna Prajna school

Figure 1 Typical PoC Enrolment location

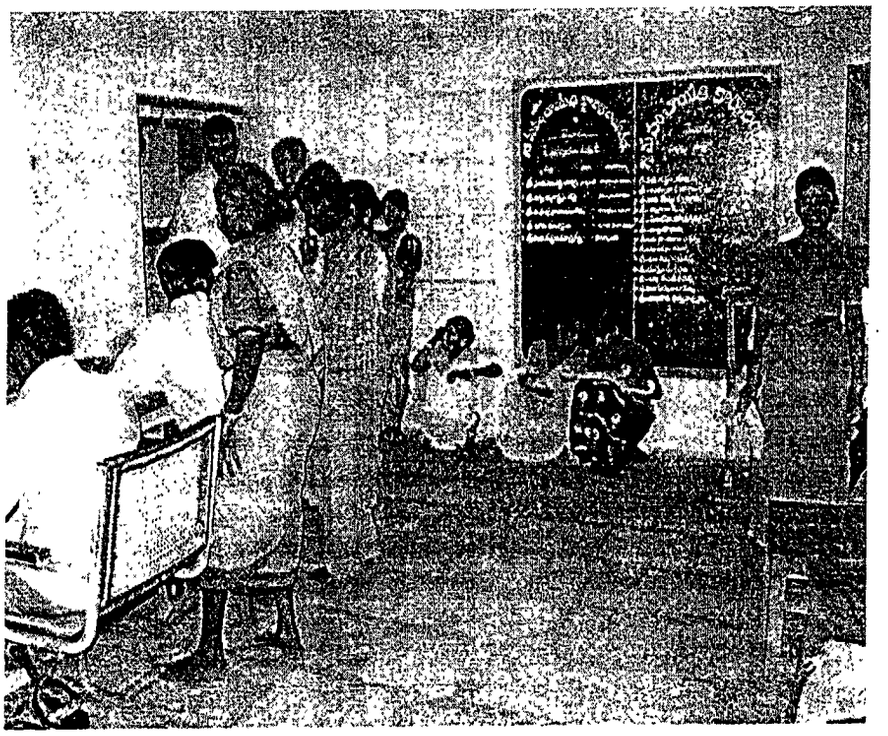


Figure 2 Typical PoC Enrolment room

Biometric devices

Fingerprint scanners and iris capture devices from three different vendors were used in the three PoC states. In Karnataka, the iris devices were from Iris ID (formerly LG Iris) and the fingerprint devices were from Morpho (formerly Sagem). In Bihar, the fingerprint scanner and the iris capture device were both from Crossmatch Technologies. In Andhra Pradesh, the fingerprint scanner and iris capture devices were both from L-1 Identity solutions. In Andhra Pradesh, both a single-eye iris capture device and a two-eye iris capture device were used. The Crossmatch iris devices were binocular type, the L-1 iris devices were hand-held, and the Iris ID iris devices were mounted on tripods, but could also be used as hand-held devices Using multiple devices added further to the diversity of the PoC process and later enabled us to match images captured using different devices.

Preparation of enrolment agency and software

Enrolment agencies who had already worked with the respective states on previous projects were chosen to implement the PoC by the respective state government agencies. The agencies were 4G ID solutions in Andhra Pradesh, Comat Technologies in Karnataka, and SmarTech Technologies (an arm of Glodyne) in Bihar. In parallel, biometric devices were procured for the PoC. The biometric devices procured were the following: iris capture devices, iris and face capture devices, slap fingerprint scanners, and single finger capture devices.

The enrolment agencies had varying levels of biometric enrolment experience. The UID technology group worked with each agency to ensure adequate training and prescribed the process flow to be followed.

A reference implementation of the enrolment software was created to standardize the process and have a uniform look-and-feel of the application across all three states. However, since the devices used were different in each state, the enrolment software used in each state was a custom version which followed the reference design. The UID technology team worked with each of the three agencies to create the customized software to be used in the corresponding state. There were also variations in the capture process followed, particularly in iris capture, because of the variations in capture devices.

A special feature of the enrolment software was that all biometric images went through a software quality check process. The quality check would indicate a pass or fail based on minimal acceptable quality of the image. If the quality check failed, the image would still be stored, but the operator would be required to recapture the image. The enrolment software entailed the operator to repeat the capture up to four times. The software ensured that the operator was not able to proceed to the next step until the recapture was done.

One important aspect of the enrolment software was the capture of process data along with biometric and demographic data. Thus the number of capture attempts and timestamps captured at numerous points in the capture process were written into an XML file during enrolment. This enabled us to eventually carry out a detailed analysis of the process.

Pre-enrolment field and data preparation

The initial step was to work with the local authorities to find possible enrolment locations and make preparations for getting people to show up. The local authorities typically went house-to-house to inform residents about the date and time they were to enrol. The authorities would also be present at the enrolment centre to ensure that people did show up, resolve any disputes among the enrolees and maintain order. The part played by the local authorities was consequently crucial to the success of the enrolment drive.

The enrolment agency supervisors visited the locations to identify the most suitable building for the enrolment centre, ahead of the start of the PoC. They also arranged for the right furniture among what was available in the building and set up the enrolment stations to meet the PoC needs. One important point was that the table should not be too wide and the heights of the operator, and size of the chairs for the enrolee should accommodate the biometric capture process.

Additionally, it was ensured that there was adequate space for people to wait outside since people crowding around the biometric stations would disturb the process. However, a few chairs were kept nearby for observers since it was felt that each resident observing the process before his or her enrolment would improve the person's ease of enrolment. Posters describing the biometric process (shown in photograph below) were also put up at the door of the enrolment centre to help enrolees familiarize themselves with the process.

In parallel, the demographic data of the residents of the local taluk or mandal was obtained from the food and civil supplies department and loaded into the appropriate laptops. Blank

forms were also kept at the enrolling centres to accommodate people who did not appear in the database, but wished to enrol.

Provisions were made for a bucket of water and towels for residents involved in manual work to clean their hands before enrolment. Also wet and dry clothes were kept at each enrolment station for assisting people with overly dry fingers.

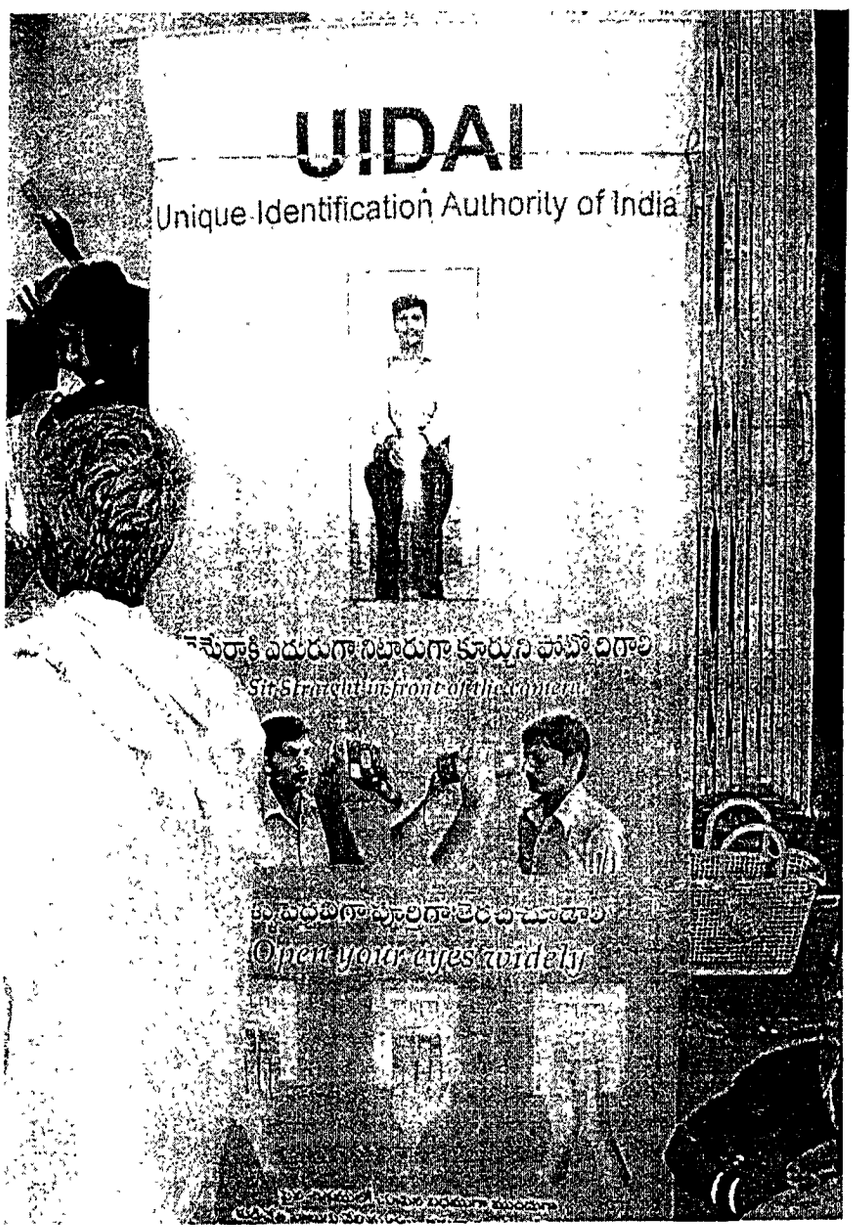


Figure 3 Poster describing biometric capture for residents to observe

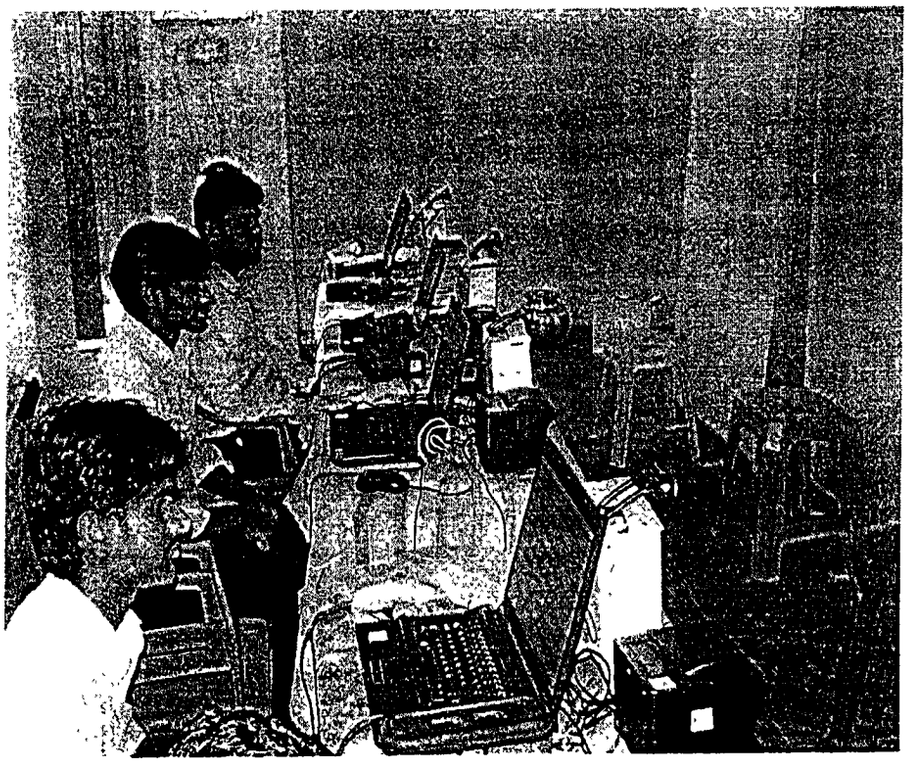


Figure 4 Enrolment stations

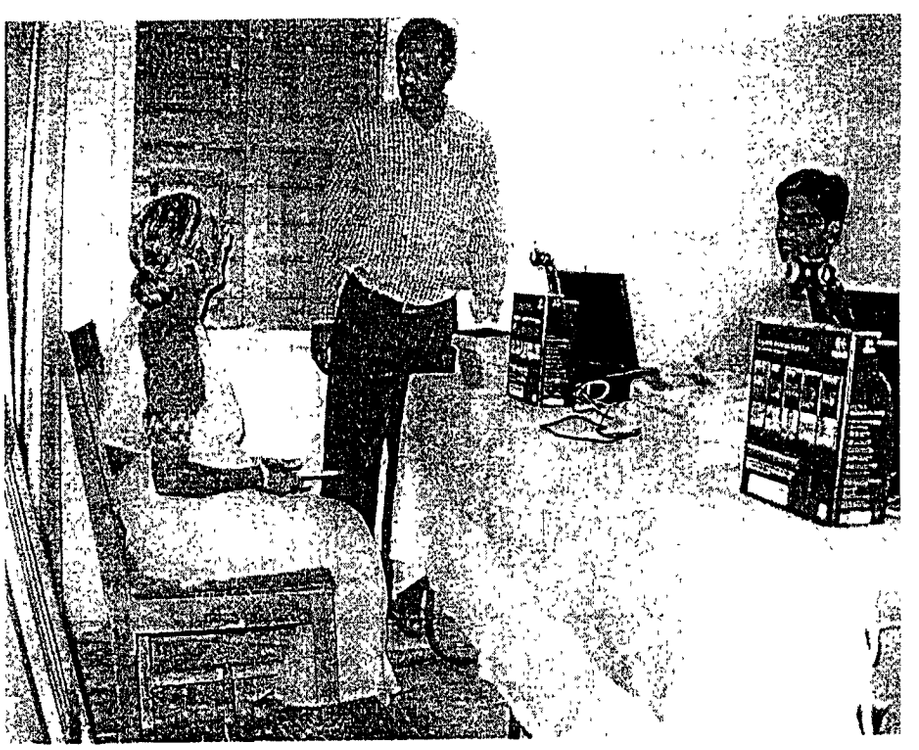


Figure 5 Enrolment station

Enrolment Process

The basic process and associated workflow enforced by the enrolment software is described below. There were minor variations in each state due to the different devices used and the differences in demographic data collection; these variations are listed subsequently.

1. The enrolee would arrive at the enrolling centre with an identifying card. The first station was a non-biometric station where the demographic information of the enrolee was either collected from the card or retrieved from an existing database. A form populated with the demographic information was then printed (or in some cases, forms were printed ahead of time) and any necessary corrections made. The demographic information collected was name, address, date of birth (or age), and occupation.
   During the second round of enrolment, the tear-off receipt (described in step 6) was used to identify the application number of the applicant.
   Following this the enrolee was sent to an available biometric enrolment station.

2. Using the application number from the application form or first round receipt, the enrolee's demographic record was populated in the enrolment screen. At this point, the operator would check for biometric exceptions (missing fingers or eyes) by asking the enrolee to show his/her hands. If there was an exception, it would be marked in the exception section of the screen, and the information would be stored in the XML file along with the demographic information.

3. Once the above process was completed, the biometric capture would start. The enrolee would first sit down facing the operator and the face photo would be captured by a webcam. The enrolment software would then perform a quality check and crop the image. If the quality check or image cropping failed, the photo would be recaptured up to a maximum of four total attempts. The cropped face photo would be shown on a small frame on the right and it would remain on display during the rest of the biometric capture (see Annexure 1 for screen shots).

   A white non-reflecting background screen was placed behind the enrolee's chair to provide a uniform background for face photo capture, and ensure that the background portion of the photo quality check was met. While capturing face photo, the enrolee was instructed to look straight and keep his or her mouth closed.

   During the second round of enrolment, the face photo from the first round of enrolment would appear on the application screen so that the operator could confirm that the same person whose biometrics had been captured in the first round was being re-enrolled. After confirming that the photo matched the enrolee, the operator would capture a new face photo which would be cropped, and replace the earlier photo on the screen. The photo would be stored along with the other biometrics in the second round database.

4. The iris images of the enrolee were captured with a single-eye or two-eye iris capture device. Based on the results of the quality check, the images would be recaptured for a maximum of four total attempts. While capturing iris image, the enrolee was instructed to look straight into the LEDs, rectangle or other appropriate point (depending on the device), open his or her eyes wide ("look angry or glare") and to not blink.

5. The three slap fingerprint images (4-4-2), i.e left hand slap, right hand slap, and slap image of the two thumbs, were captured. As above, based on the results of the quality check, the capture would be attempted up to four times. The slap fingerprint capture was done with the enrolee standing. This was to ensure that the person could apply sufficient pressure to be able to get good fingerprints. While capturing fingerprint images, the enrolee was instructed to open their hands, place their fingers flat on the platen in the correct position and press their fingers down firmly.

6. Individual fingerprints of all ten fingers were captured using a single-finger capture device. The individual prints were matched with the corresponding prints from the segmented images of the slap fingerprint captured in step 4. If the fingerprints did not match, step 5 was repeated, while still not exceeding a total of four slap attempts for each type of slap capture. This capture was also done with the enrolee standing.

7. If one or more of the enrolee's fingers or eyes were missing, an exception photograph of the enrolee's face along with both hands opened to show the missing fingers would be captured. This was in order to have a visual record of the missing biometrics.

8. In the first round of enrolment, a tear-off receipt that was printed at the bottom of the application form was given to the enrolee, and the enrolee was asked to bring the tear-off receipt when returning for re-enrolmert in the second round.

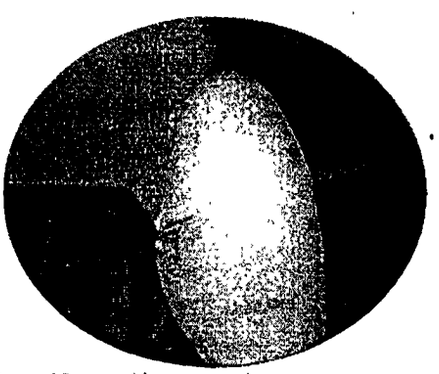


Figure 6 Damaged finger example

Figure 7 Damaged eye example

Process Variations

1. Identifying document of enrolee: The enrolee would come to the enrolling centre with his or her ration card in the case of Karnataka and Andhra Pradesh. In Bihar, the enrolee was asked to bring his or her job card. Neither of these cards would completely identify the individual since a single ration card listed all members of the family and each job card would list all adult members of the family. So, an additional digit was appended to the ration card or job card number to create an application number identifying the individual.

   Collection of demographic information: In Karnataka, a pre-printed form which had the relevant data for the enrolee was chosen from a stack containing forms for all residents of the village sorted by ration card number. This was handed to the enrolee. In Andhra Pradesh, a form containing the enrolee information was printed at the enrolment site and handed over to the enrolee. In Bihar, the enrolees were asked to fill in the form (if necessary, the enrolment agency employee filled the form for the enrolee) and the data was then entered into the application.

2. For iris capture, there were three variations in the three states:
   In Bihar, a binocular type iris capture device was used. Ideally, the enrolees would be able to hold the iris device to their eyes unassisted, and wait for the iris capture to complete. In practice, the operator sometimes helped hold the device up, particularly in the case of older enrolees.

   In Andhra Pradesh, the operator held the device. The enrolee would stand up and the operator would bring the capture device close to the enrolee's face and then move the device back slowly to capture the iris image. Both single eye devices and dual eye devices were used. Dual eye device were used for about 61.5 percent of the enrolments and the remaining were done used the single eye device.

   In Karnataka, a dual eye device was used and it was mounted on a tripod for a large part of the PoC. The resident would move his or her face slowly towards the device and the device would capture the iris image at the appropriate distance. A small portion of the PoC was done using the iris capture device as a hand-held device, where the operator moved the device towards the enrolee's eyes The PoC done later in the school in Karnataka also used the same dual eye device as a hand held device.

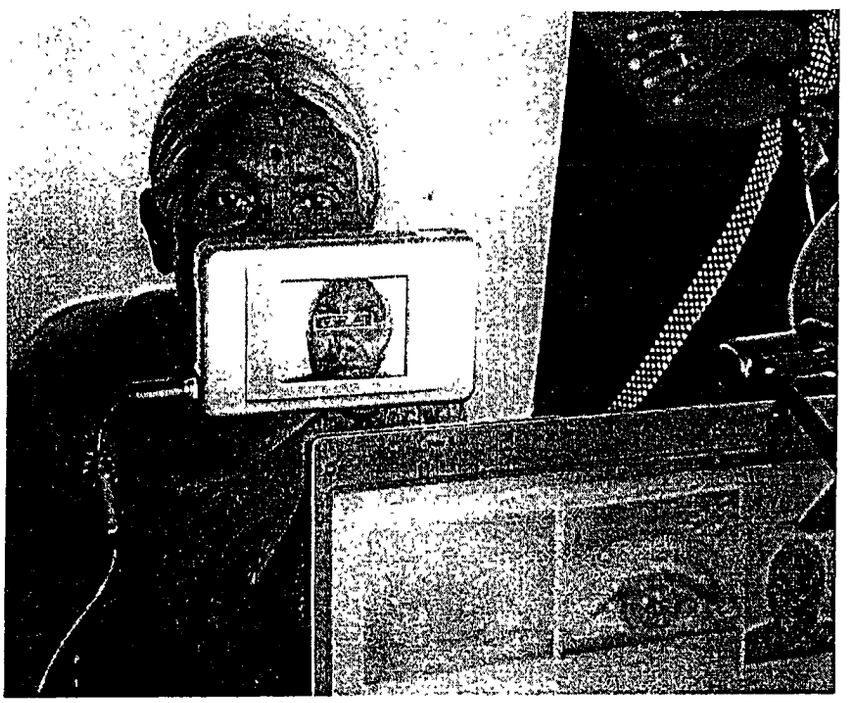


Figure 8: Karnataka- iris camera mounted on a tripod

Enrolment software

The enrolment software had the following screens (Annexure 1)

1. Demographic data and biometric exception capture
2. Face photo capture
3. Dual iris capture
4. Slap fingerprint capture – three slaps to capture all ten fingerprints
5. Capture of ten fingerprints using a single finger device
6. Capture of an exception photograph if necessary

The following are a few noteworthy points related to the enrolment software:

Once the face photo was captured and cropped, it was displayed on a small frame during the capture of all the other biometrics. This would allow the operator to avoid mistakes and avoid combining the biometrics of two different individuals in one enrolment if there was an interruption halfway through the enrolment process.

There were visual biometric quality indicators associated with each image, which the operator could use to quickly gauge image quality (Annexure 1). This was done to avoid the necessity for the operator to interpret quantitative scores.

The following are the actual re-enrolment rates observed.

Karnataka Re-enrolment Rates

	Taluk	Gram Panchayath	Enrolment numbers	Reenrolment numbers	Percentage reenrolling
Tumkur	Tumkur	Bellavi	1,976	1,692	86%
Tumkur	Gobi	Chelur	2,262	1,947	86%
Tumkur	Madhugiri	Doddery	2,193	1,797	82%
Tumkur	Tiptur	Kibbanahalli	2,548	2,171	85%
Tumkur	Sira	Bukkapatna	2,267	1,615	71%
Mysore	Mysore	Varuna	2,283	2,097	92%
Mysore	HD Kote	Hommaragalli	2,698	2,510	93%
Mysore	Nanjangud	Hadinaaru	1,908	1,659	87%
Mysore	Hunsur	Gowdagere	2,728	2,454	90%
Mysore	KR Nagar	Tippuru	2,754	2,331	85%
		Karnataka Total	23,859	20,079	84%

Andhra Pradesh Re-enrolment Rates

District	Mandal	Village	Enrolment numbers	Reenrolment numbers	Percentage re-enroling
Medak	Tupran	Ghanpur	2000	1819	91%
	Wargal	Wargal	2435	2123	87%
	Wargal	Veluru	2095	1978	94%
	Chegunta	Narsingi	2756	2539	92%
	Patancheru	Ward-11	2602	1187	46%
Krishna	Mylavaram	Velvadam	2826	2477	88%
	Kruthivennu	Lakshmi puram	2481	2169	87%
	Vijayawada Rural	Nidamanuru	3051	2659	88%
	Penamaluru	Poranki	3114	2532	81%
	Vijaywada Urban	Ward 9	2377	1200	50%
		AP Total	25717	20683	80%

Observations

The following are the observed average capture times and number of attempts

		Face photo	Iris	Slap Fingerprints (three images)
Adults	Capture times (for all attempts combined)	34 seconds	52 seconds	1 minute 51 seconds
Adults	Number of attempts	1.5	1.9	1.5
Children (4 to 15 years)	Capture times (for all attempts combined)	33 seconds	35 seconds	1 minute 13 seconds
Children (4 to 15 years)	Number of attempts	1.4	3.1	1.4

The important process time averages are as shown below:

Average biometric enrolment time for adults is 3 minutes 17 seconds

Average biometric enrolment time for children (4 to 15 years) is 2 minutes 21 seconds

Capture times analyzed by age, occupation, and gender are listed in Annexure 2

	Percentage of enrolees
One or more fingers missing or otherwise not capturable	1.2 %
Either or both eyes missing or otherwise not capturable	0.5 %
Missing all 10 finger and both eyes	0.01 %

Table: Biometric Exceptions (missing eyes and fingers)

The average time required for capture of face photo, fingerprints of ten fingers and iris image of adults was three minutes and seventeen seconds. Of this, a little over half the time was spent on fingerprint capture. The time for iris capture was a little below one minute, and face photo capture took over half a minute. The iris image capture time varied significantly by age, with people above eighty taking twice as long as people in their twenties. The variation in capture time of fingerprints was lower with the older group taking twenty percent longer than the younger group. One apparent anomaly in fingerprint capture times is that 20 to 30 year old people took longer to have their fingerprint captured than older people. This can possibly be attributed to the fact that they may be engaged in occupations involving heavier physical labour and correspondingly more wear on their fingerprints than their older

counterparts. The average capture time for iris images and fingerprints for children were no worse than that for adults. This included the youngest children who were only four years old.

The enrolment time also showed significant variation by occupation, with the occupations involving physical labour showing longer enrolment times. For example, agricultural labourers took about one-third longer to have their fingerprints captured compared with public and private sector employees and other white collar workers. Similarly, for iris capture, the variation was over thirty percent.

There were many blind people who had their iris captured successfully. This was because even though they were blind, their iris was intact. Similarly, many people with worn fingerprints had their fingerprints successfully captured. The table above shows that the percentage of residents enrolled with one or more missing fingers was only a little over one percent and the percentage of enrolees with one or both eyes missing was less than one percent of the total enrolee population.

The enrolment PoC for children showed that the process of enrolling children in the age range of four to fifteen was not significantly harder than that of enrolling adults.

Process observations

An important conclusion reached was that the best possible way for conducting biometric enrolment was to have the enrolee be stationary and have the operator do the positioning of the device.

It was also clear that the operator instructions to the resident were very important. The best results obtained in terms of quality and efficiency was when the operator spent a few seconds *ahead of* each biometric capture clearly explaining what was required on the part of the enrolee, for example "keep eyes wide open", "keep fingers flat on the platen and press hard", etc. This was much more effective than trying to correct the enrolee's gaze, positioning etc. *during* the capture of the biometric.

The use of quality check software clearly helped in two ways. The first was that there was a clear message that quality of data collected mattered to the UIDAI and that the quality was going to be monitored. The second was that the operator began to recognize good quality images and over time was well versed in collecting high quality images.

The physical layout of the devices and the ability of the operator to reach out and help the enrolee as required were also seen to be important. Therefore the width of the table had to be small enough so that the operator could reach across. The other option was that the enrolee stood next to the operator on the right side for fingerprint capture.

The ambient light was not always sufficient to capture good quality face photographs even during the day. Table lamps or other artificial lighting was often needed.

The mobile USB tethered iris devices used were adequate for capturing good quality images. In addition, fingerprint images from different devices were matched and there were no

compatibility issues in doing the matching. In general, the devices worked as expected. The differences in process were much more significant compared to the differences in devices.

Iris enrolment was eminently possible from the operator's perspective and was also well accepted by the enrolee. In fact, the iris capture took less time than fingerprint capture.

Older people sometimes needed assistance in positioning themselves (see picture below) and often required assistance in pressing their fingers hard enough on the platen to get good fingerprints. Children were able to position themselves correctly and maintain the position long enough for successful capture of all three biometrics.

The PoC was conducted in the summer months of April, May and June in Medak district of Andhra Pradesh and in Nalanda district in Bihar. During a few days when the PoC was in progress, the temperature reached 44 degrees Celsius in Nalanda district. Despite the extreme temperature and the fact that no fans were available, enrolment went on normally.

In conclusion, it is clear that it is possible to collect good quality biometrics in rural India despite existing shortages in infrastructure, and the biometric variations within the rural population. Reasonable processes can be specified to undertake enrolment on a much larger scale

Figure 9: Older resident being assisted with slap fingerprint capture

Figure 10: Eighty six year old resident being assisted with iris capture

Biometric observations

The ultimate goals of biometric enrolment for the UIDAI are two-fold. One is to carry out biometric deduplication for all enrolees in India, and the second is to authenticate the biometrics of an enrolled resident on demand. Therefore, these activities have been the focus of the analysis conducted on the PoC data.

Biometric matchability analysis was done on the PoC data to understand the quality of the data and how well it could be used for deduplication and authentication. The basic tool used to study the results is the ROC (Receiver Operational Curve) which shows how two types of potential errors can be traded off against each other for the given set of data. Two of the ROC curves that were obtained from the analysis are shown in Annexure 3 to show a sample of the analysis and to explain the results. The analysis was done using images of ten fingerprints and two irises. The face biometric was not used for matching.

Terminology

The following terminology is needed to understand the results.

Identification: This is the process where any one person's biometrics is matched with that of *all* the other people in the database. This results in establishing the enrolee's biometrics as either unique or as a likely duplicate of the biometrics of an enrolee who had enrolled earlier.

FPIR: False Positive Identification Rate: This is the likelihood that a person's biometrics is seen as a duplicate (i.e., the biometric deduplication software identifies his biometrics as matching with that of a different person), even though it is not a duplicate in reality.

FNIR: False Negative Identification Rate: This is the likelihood that a person enrols a second time and the deduplication software is unable to identify their biometrics as a duplicate set.

Verification: This is the process where a person's biometrics is compared only with a copy of his or her biometrics that was captured earlier.

FAR: False Accept Rate: This is the likelihood that a person's biometrics is matched against a different person and the biometrics is seen to match, i.e. the person is wrongly seen to be a different person.

FRR: False Reject Rate: This is the likelihood that a person's biometrics does not match against an earlier sample of his or her biometrics and so he or she is not recognized as the same person.

Results

The matching analysis was done on two sets of 20,000 biometrics, for a total of 40,000. However, the number of comparisons was several orders of magnitude more than 40,000, since each set of fingerprints would be matched against every other set of fingerprints in the data set. Similarly, the iris images from each person would be matched against that of every other person in the data set. Therefore, the results are statistically significant and can be extended to larger populations.

We will now compile the data on the accuracy obtained by enrolling with only fingerprints, enrolling with only iris images, and by enrolling with both biometrics. We will do so using the Identification ROC curve shown in Appendix 3. To compare the accuracies in these three cases, we will look at the point where the FPIR (i.e. the possibility that a person is mistaken to be a different person) is 0.0025 %.

Comparing the FNIR numbers achieved, the FNIR using two irises only is 0.5%, that achieved by using ten fingers only is 0.25%, and that achieved by using ten fingers and two irises is 0.01%. The conclusion we can draw is that accuracy achievable using ten fingerprints is twice that of the accuracy achieved using iris images. Even more important, the accuracy achieved by using ten fingerprints and two irises is fifty times better than by using irises alone and twenty five times better than by using fingerprints alone. The accuracy level achieved was 99.99% in this case.

Looking at the verification ROC for children and adults, we can see that the accuracy obtained in matching for children using iris is better than that for adults. Similarly, the accuracy obtained using fingerprints is better for children than for adults..

By doing analysis as shown in the examples above on real data captured under typical Indian conditions in rural India, we can be confident that biometric matching can be used on a wider

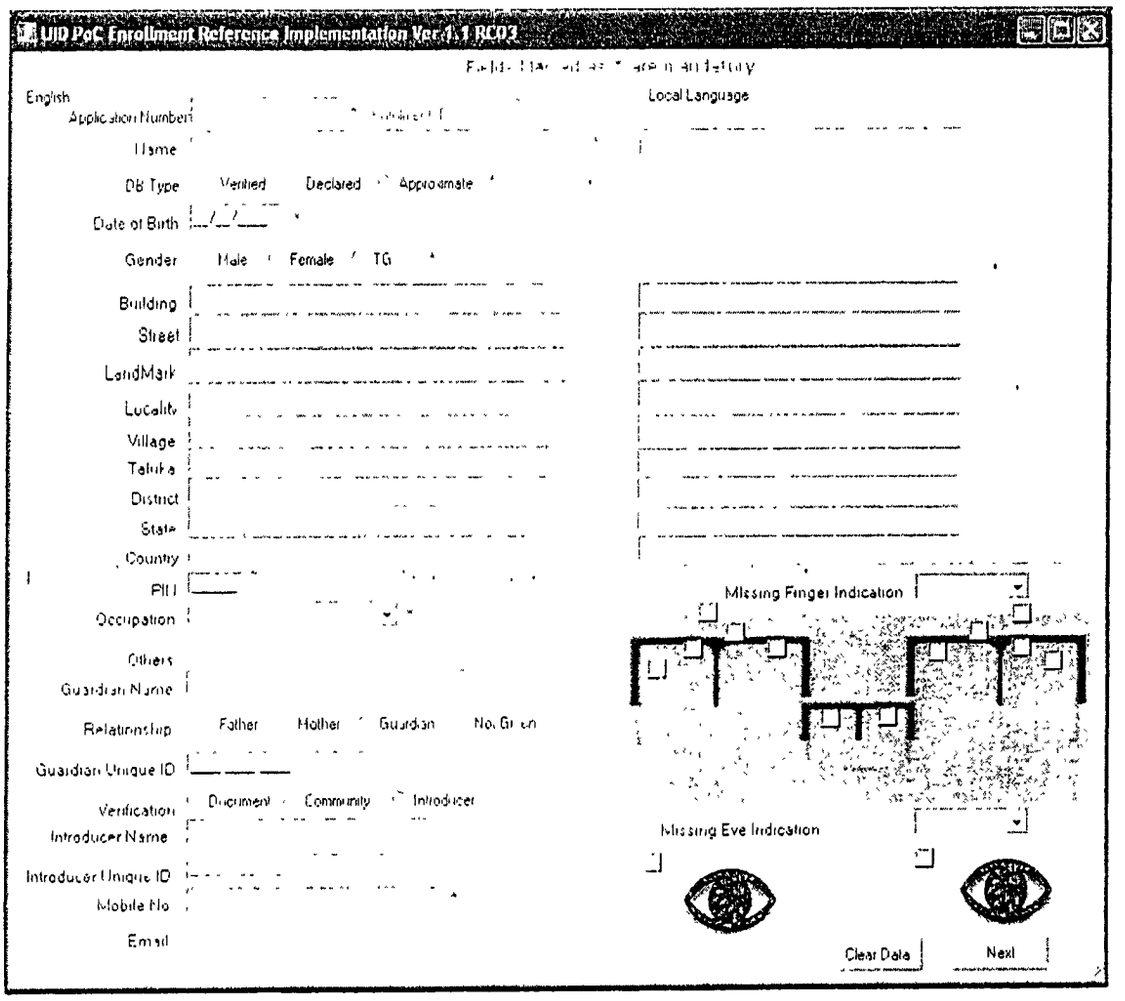
scale to realize the goal of creating unique identities. We have further confirmed that is true as much for children as for adults.

Conclusion

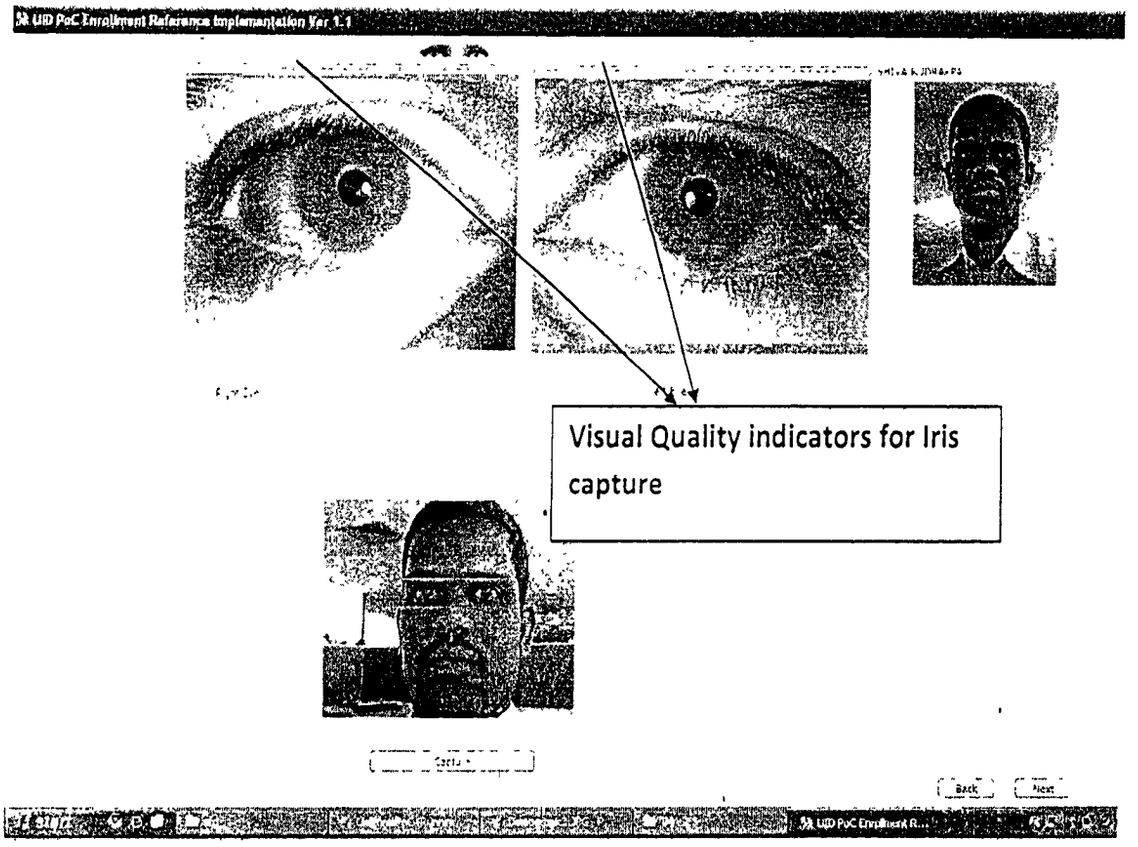
The PoC study was a useful precursor to large scale UID enrolment and has validated our hypotheses regarding biometric enrolment. Iris enrolment was not particularly difficult, and dramatically improved the accuracy levels that could be achieved. The biometric accuracy levels necessary for deduplication of all residents of India are achievable. The time needed for capture of biometrics in typical rural conditions is small enough to support large scale enrolment. In conclusion, the PoC study was a productive part of the ongoing rollout of the UID program.

Annexure 1 - Enrolment application screen shots

Demographic screen with exception indicators

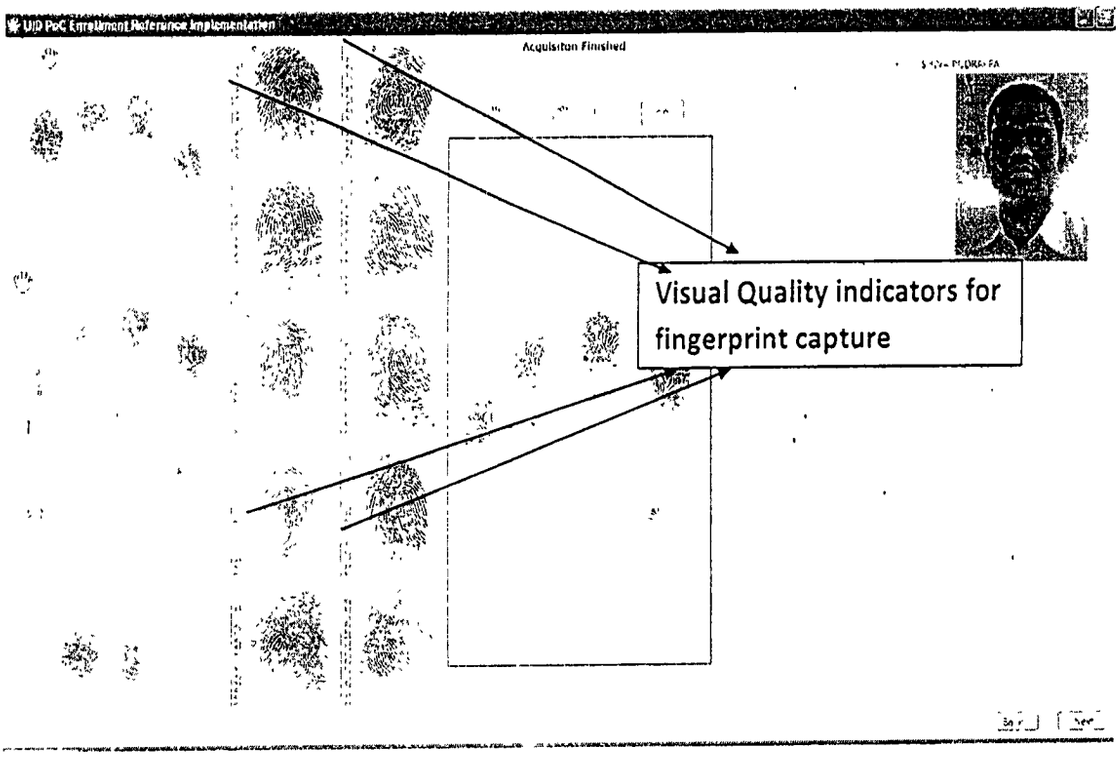


Iris Capture Screen with quality indicators highlighted

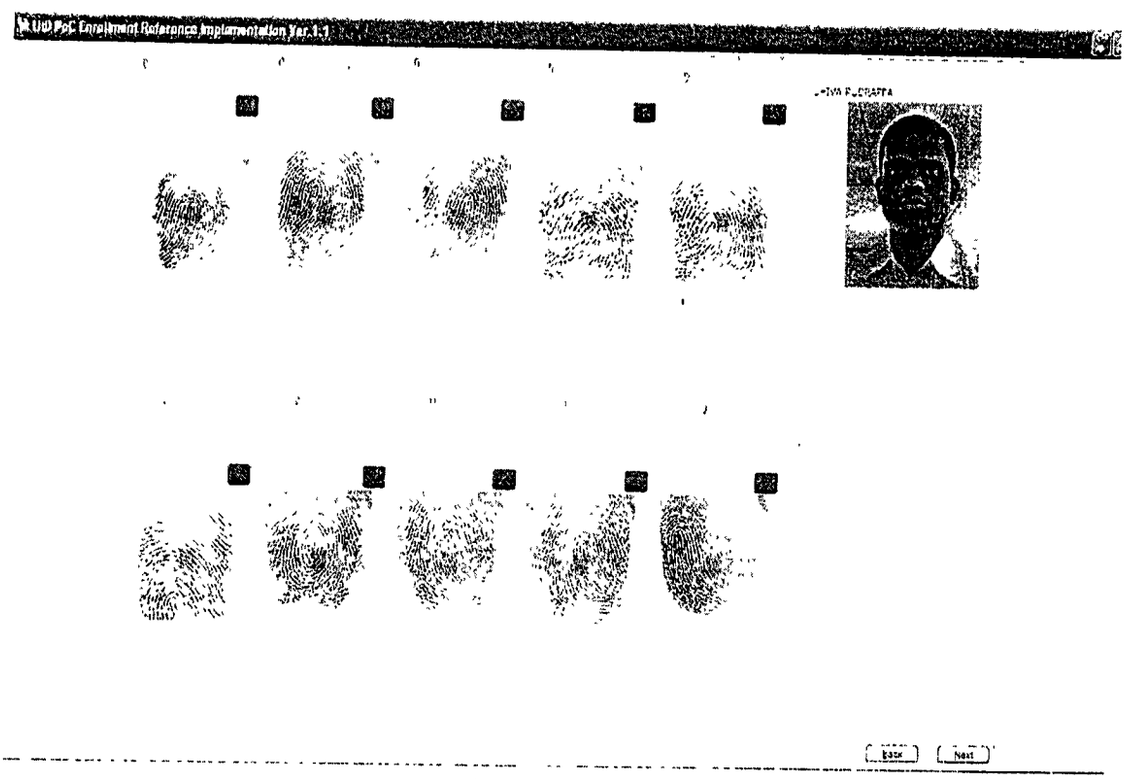


~~243~~
242

Fingerprint Capture Screen with quality indicators highlighted



Single Fingerprint Capture Screen



Annexure 2 – Enrolment times by age and demographics

Age	Under 20	20 to 30	30 to 40	40 to 50	50 to 60	60 to 70	70 to 80	Above 80
Face	0:00:31	0:00:31	0:00:33	0:00:35	0:00:37	0:00:38	0:00:40	0:00:43
Iris	0:00:42	0:00:42	0:00:49	0:00:54	0:00:58	0:01:07	0:01:15	0:01:24
Fingerprint	0:01:45	0:01:52	0:01:43	0:01:45	0:01:53	0:01:56	0:02:08	0:02:14

Enrolment times by age

Occupation	face	iris	slap	Total
Agriculture Labour	0:00:27	0:00:53	0:02:11	0:03:31
Employee	0:00:27	0:00:39	0:01:36	0:02:43
Daily wage earner	0:00:25	0:00:46	0:02:03	0:03:14
Student	0:00:22	0:00:37	0:01:49	0:02:49
House Wife	0:00:27	0:00:59	0:02:04	0:03:29
Coolie	0:00:55	0:00:48	0:01:28	0:03:11
Farmer	0:00:43	0:00:51	0:01:41	0:03:15
Beedi Worker	0:00:21	0:00:44	0:02:57	0:04:02
Artisan	0:00:22	0:00:42	0:03:20	0:04:24
Driver	0:00:33	0:00:39	0:01:52	0:03:04
Other	0:00:27	0:00:44	0:02:16	0:03:27
Retired	0:00:28	0:01:40	0:02:08	0:04:16
Rickshaw Puller	0:00:24	0:00:37	0:01:34	0:02:35

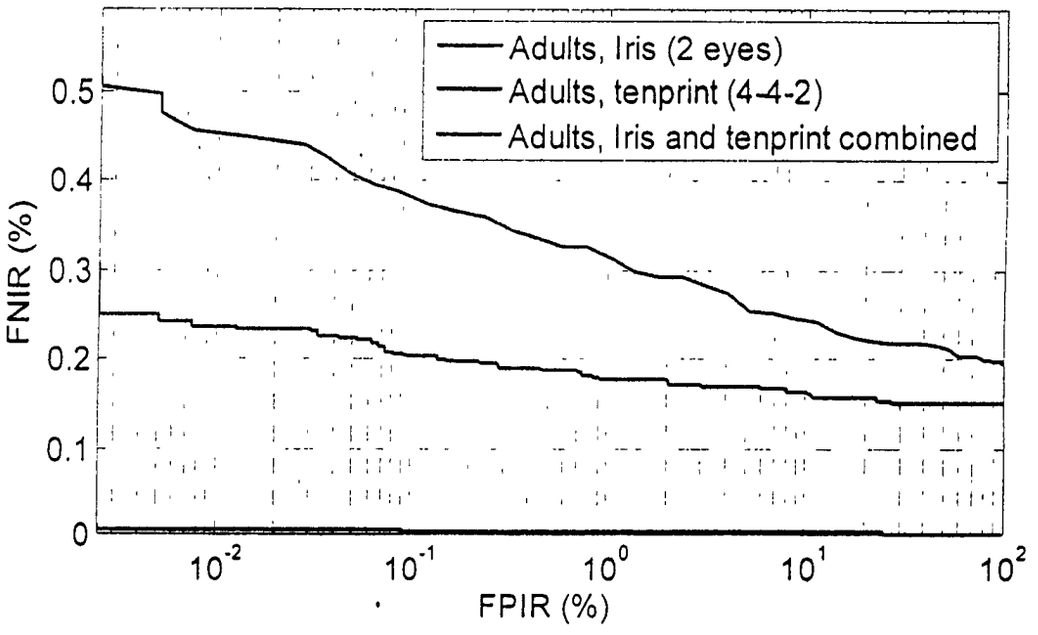
Enrolment times by occupation

	face	iris	slap	total
Male	0:00:30	0:00:48	0:01:50	0:03:08
Female	0:00:27	0:00:56	0:02:09	0:03:32

Enrolment times by gender

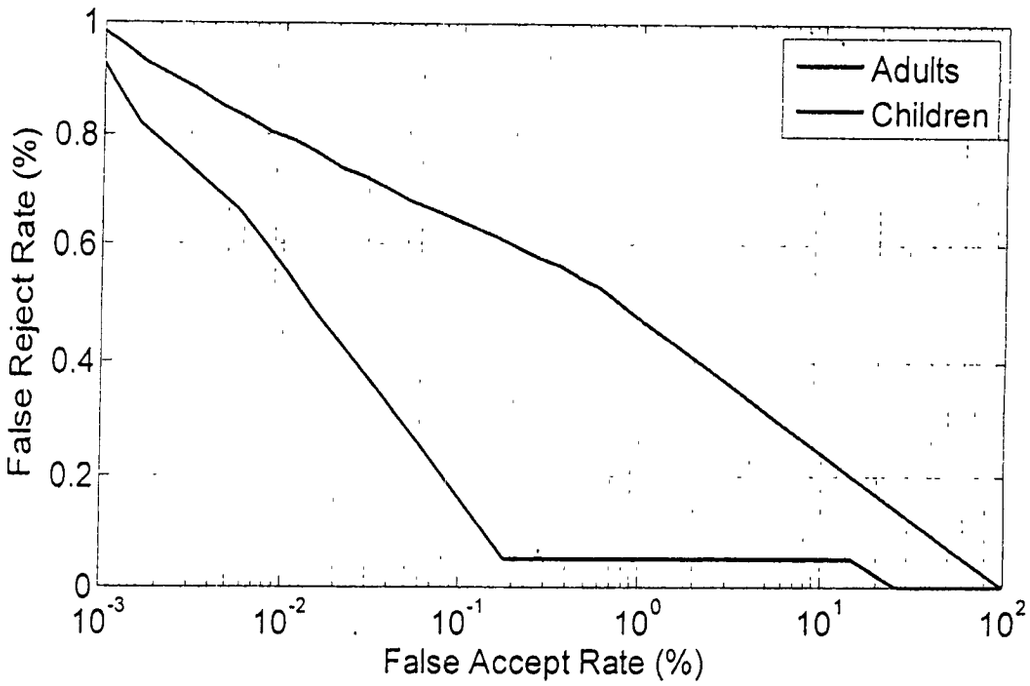
Annexure 3 – Biometric matching accuracy curves

Identification ROCs(1 in 20,000) for adults

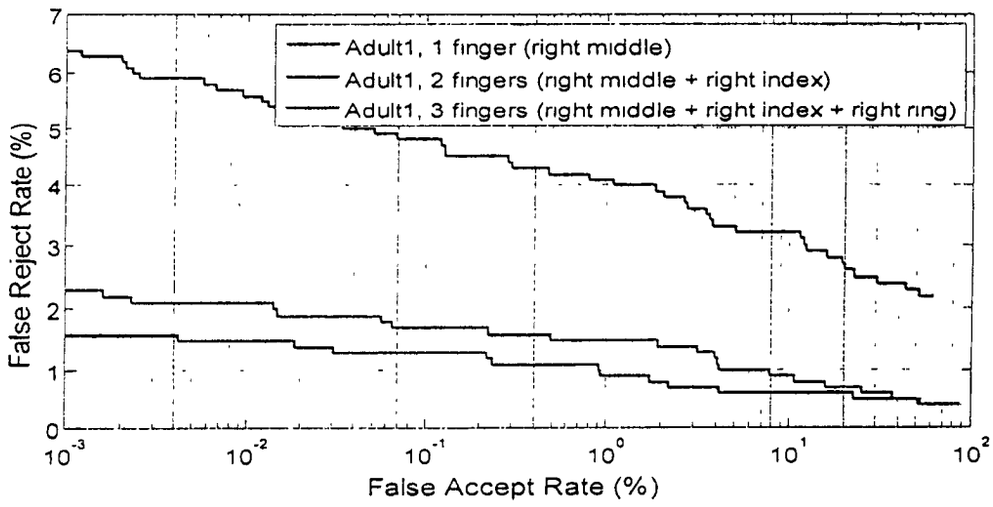


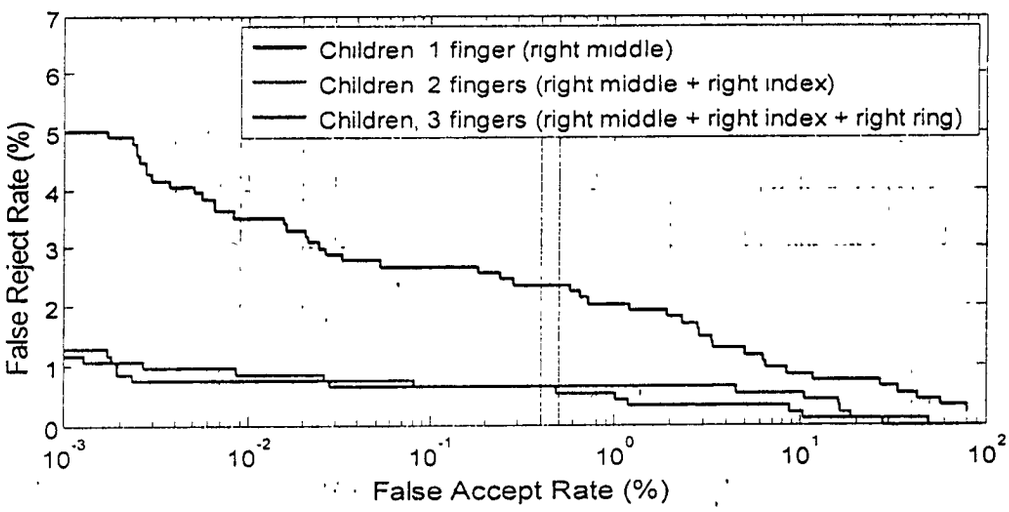
~~247~~
246

Iris identification ROCs (1:1) for adults and children



Verification ROC for 1,000 children and adults





GLOSSARY OF TERMS

Aadhaar - Unique Identification Number

ATM - Automated Teller Machine

Authentication - The process of verifying the UID number of a resident with reference to his biometrics.

Authority - Unique Identification Authority of India (UIDAI).

"Aadhaar Authentication Services" shall mean the authentication services provided by UIDAI and used by Authentication User Agency where the personal identity information of / data of an Aadhaar-holder (who is a beneficiary, customer, employee or associate of the Authentication User Agency is matched with their personal identity information / data that is stored in the UIDAI's Central Identity Data Repository in order to provide Aadhaar enabled services to such Aadhaar holder.

API Application Programming Interface: An application programming interface (API) specifies how some software components should interact with each other.

ASA Authentication Service Agency :Authentication Service Agency. An organization or an entity providing secure leased line connectivity to UIDAI's data centres for transmitting authentication requests from various AUAs.

AUA Authentication User Agency :Authentication User Agency. An organization or an entity using Aadhaar authentication as part of its applications to provide services to residents. Example: Bank

BC- Business Correspondent: Term for banking channel for rural India.

B-FTE -Biometric Failure to Enrol :

BFD Best Finger Detection: identification of the best finger(s) to improve authentication accuracy and hence be more inclusive in supporting Aadhaar authentication across all sections of society.

BPL - Below Poverty Line

"**Biometric Information**" shall mean ten finger prints and iris image of aresident, captured by UIDAI, as a part of the enrolment process for issuanceof Aadhaar Number.

Biometric Data - refers to the facial image, iris scan and fingerprints collected by the Enrolment Agency from the enrollees based on the standards prescribed by the UIDAI and by following the process laid down for the purpose. The data collected is passed onto the UIDAI as per the process prescribed.

CSC - Common Service Centres operating as franchisees of Service Center Agency

(SCA) within a State, as part of the CSC Scheme of the National E-Governance Plan of India.

CSO - Civil Society Outreach, an invitation undertaken by UIDAI to get learnings from NGOs on issues related to Migrant labour, homeless etc.

CGHS - Central Government Health Scheme

CSV - Comma Separated Variables or values, a simple file format for Computer which is widely used due to ease.

CIDR -Central ID Data Repository: data centre/s where data of resident enrolled is stored and accessed from.

De-duplication - the process of using the Demographic and Biometric data collected from an enrollee to check against rest of the data so as to avoid duplicate enrolments.

DoB - Date of Birth

Demographic Data - refers to the personal information collected or verified by the

Enrolling Agency based on the data fields prescribed by the UIDAI and by following the process laid down for the purpose. The data collected is passed on to the UIDAI as per the process prescribed.

DIT - Department of Information Technology.

DDSVP - Demographic Data Standards and Verification Procedure :The UIDAI set up the Demographic Data Standards and Verification ProcedureCommittee (Data standards

committee) chaired by Shri N. Vittal. The Data StandardsCommittee submitted its report on December 9, 2009.

e-KYC- Electronic Know Your Customer - an electronic substitute which is instant and paperless for industry use to meet KYC requirement of Banking, Telecom etc.

ECHS – Ex-servicemen Contributory Health Scheme.

eGoM – Empowered Group of Ministers.

Enrolment – refers to the exercise of collection of demographic data after verification, collection of biometrics, and the allocation of the UID number after de-duplication.

Enrolment Centre – refers to the premises located in the area where the enrolment is being carried out. One Enrolment Centre can host multiple Enrolment Stations.

Enrolment Station – refers to an individual enrolment booth/enclosure inside the Enrolment Centre. The capture of Demographic and Biometric data is done in this Station.

FPIR -False Positive Identification Rate which describes the proportion of identification transactions by users not enrolled in the system, in which an identifier is returned.

FI- Financial Inclusion: Programme of banking industry to expand banking to rural India.

FTE- Failure to Enrol : Failure to Enroll: Failure of the biometric system to form a proper enrolment template for an end-user. The failure may be due to failure to capture the biometric sample or failure to extract template data (of sufficient quality)

G2C -Government –to- Citizen or transactions of Government which are targeted to large population.

G2G -Government-to-Government are those transactions that are with Central or State Government.

Introducer : a person of credibility and local presence who is authorised by the Registrar (Govt. And other agencies who verifies and assure identity of another resident.)

IFSC - Indian Financial System Code which is the code used by banking industry to identify a particular Branch.

IOCL - Indian Oil Corporation Ltd.

KSA: KYC Service Agency. Avalid ASA who has been approved and has signed the agreement to access KYC API through their network.

KUA: KYC User Agency. A valid AUA who has been approved and has signed the agreement to access KYC API.

KYR - Know Your Resident - On the lines of KYC of Banking Industry like eg Ration Card Number or welfare beneficiary identity number.

KYR+ - Fields required in addition to KYR fields required by the Registrars

MNREGA - Mahatma Gandhi National Rural Employment Guarantee Act

Manual - Enrolment Manual.

MoU - Memorandum of Understanding

NGO - Non Government Organization.

NPR - National Population Register, which is a programme of Registrar General of India/Census Office for enrolling and assigning ID numbers to residents.

NREGA - National Rural Employment Guarantee Act

OTP - One Time Password which is a one time personal identification number generally, sent to the mobile phone number for authentication framework.

Operator - the person employed by the Enrolment Agency and engaged in the capture of Demographic and Biometric Data.

ORGI - Office of Registrar General of India.

PoC- Proof-of-Concept - which is a programme undertaken in a smaller denomination to test the usefulness of the programme.

PoR - Proof of Relation which is used in the context of minor getting enrolled in UIDAI.

Resident - Normal resident of India.

RFP - Request for Proposal which is the term to denote tender or procurement formalities. .

RGI-Registrar General of India

RSBY - Rashtriya Swasthya Bhima Yojana

RDPR - Rural Development and Panchayati Raj

ISO International Standards Organization:ISO (International Organization for Standardization) is the world's largest developer of voluntary International Standards. International Standards give state of the art specifications for products, services and good practice, helping to make industry more efficient and effective. Developed through global consensus, they help to break down barriers to international trade

"Aadhaar Enabled Services" shall mean services provided by anAuthentication User Agency to Aadhaar Holder, using the AadhaarAuthentication Services of UIDAI.

"Aadhaar Authentication Services" shall mean the authentication services providedby UIDAI and used by Authentication User Agency where the personal identity information of / data of an Aadhaar-holder (who is a beneficiary, customer, employee or associate of the Authentication User Agency is matched with their personal identity information / data that is stored in the UIDAI's Central Identity Data Repository in order to provide Aadhaar enabled services to such Aadhaar holder

"Aadhaar Holder" shall mean an individual who holds an Aadhaar Number.

"Aadhaar Number" shall mean the unique identification number issued to a resident by UIDAI

Authentication Data Packet" shall mean a data packet which has been created based on pre-defined protocol (data elements, order of data elements, etc), prescribed by UIDAI from time to time and which containsPersonal Identity Data (PID) collected from Aadhaar Holders for thepurpose of Aadhaar Authentication.

"Authentication Device" shall mean a terminal or device from where theAuthentication User Agency carries out its service/business functions andinteracts

with Aadhaar Holders, by seeking authentication of AadhaarHolders identity to enable the Authentication User Agency's businessfunction.

"**Personal Identity Data (PID)**" Aadhaar-based Personal Identity Data /Information including biometric and demographic information as well as the OTPused for Authentication

OTP- One Time PIN : Personal identification number, sent generally to mobile phone number for authentication framework

RBI -Reserve Bank of India

STQC- Standardisation Testing and Quality Certification : Directorate Standardisation Testing and Quality Certification (STQC) Directorate is an attached office of the Department of Electronics and Information Technology(DeitY), Government of India, provides quality assurance services in the area of Electronics and IT through countrywide network of laboratories and centres.

TIN - Temporary Identification Number provided by RGI

UIDAI- Unique Identification Authority of India

UID - Unique Identification

UNICODE – Globally accepted standard definition of local language characters in a computer system. Character sets defined by Unicode Consortium.

USB – Universal Serial Bus

***